ComConsult Research

Der Netzwerk Insider

Mai 2014

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

Enterprise App Stores

von Dipl.-Inform. Dominik Franke

Der Markt mobiler Endgeräte boomt bereits seit Jahren und ein Abflachen des andauernden Trends ist nicht abzusehen. Während der Consumer-Markt in manchen geographischen Gebieten langsam beginnt Sättigungserscheinungen zu zeigen, werden anderorts neue Märkte erschlossen.

In all diesem Trubel und schnellen Wandel wundert es kaum jemanden, dass keine CDs oder DVDs mit Software mehr durch die Abteilungen gereicht werden. Insbesondere im mobilen Umfeld kann man mit solchen Medien überhaupt nichts mehr anfangen.

Software für mobile Endgeräte wie Smartphones, Tablets und Phablets, sogenannte „Apps“, werden heutzutage nicht über traditionelle Trägermedien übertragen, sondern über „App Stores“. Jeder Smartphone-Benutzer kennt diese App Stores und kann sie vom ersten Tag an bedienen. Kaum jemand hinterfragt diese Technik, wie sie sich so weit und still verbreiten konnte und insbesondere, was sie für ein Unternehmen mit mobilen Endgeräten bedeutet. Dieser Artikel beschäftigt sich mit der Verwendung von App Stores im Unternehmensumfeld und beleuchtet sowohl die Vor- als auch Nachteile die eine solche Lösung mit sich bringt. Zudem werden App Store-Lösungen für den Unternehmensbereich diskutiert, sowie Auswir-kungen einer Implementierung von App Stores in der Unternehmens-IT analysiert.

weiter auf Seite 6

Zweitthema

Vernetzte Hypervisor - Ein Einblick in virtuelle Switches im RZ-Umfeld

von Dipl.-Inform. Sebastian Jansen

Servervirtualisierung ist aus heutigen Rechenzentren kaum noch wegzudenken. Aspekte wie Flexibilität bei Verfügbarkeit, Skalierbarkeit und Provisionierung spielen bei der Entscheidung für oder wider Virtualisierung eine entscheidende Rolle. Doch mit einer ständig wachsenden Zahl virtueller Maschinen stellt sich zunehmend die Frage, wie man diese Maschinen adäquat in existierende Netze einbindet. Hersteller von Virtualisierungslösungen geben die Antwort: Switch-Virtualisierung direkt im Hypervisor.

1. Einleitung

Seit ihren Ursprüngen im Umfeld der Mainframes der 60er Jahre hat die Virtualisierung einen langen Weg hinter sich gebracht. Heutzutage erstreckt sich Virtualisierung nicht nur auf verschiedene Benutzersessions auf einem System, sondern erlaubt neben der virtuellen Ausführung ganzer Systeme und Desktoparbeitsplätze auch die Virtualisierung von Speicherlösungen und Netzwerkbestandteilen. Während letzteres einerseits bei Themen wie Mandantenfähigkeit und Zonenbildung eine Rolle spielt, setzt hier auch die Frage nach der Anbindung virtueller Maschinen (virtual machines - VMs) an das oder die lokalen Netze an.

weiter Seite 18

Geleit

Kampf um die Cloud: Kosten kontra Funktionalität

auf Seite 2

Mobile Devices-Spezial

Sonderaktion im Mai ComConsult-Study.tv

auf Seite 15

Standpunkt

Das Ende des Intranet

aud Seite 16

Aktuelles Intensiv-Seminar

ComConsult Sommerschule 2014

ab Seite 4

Neues Seminar

Sonderveranstaltung: Internet of Things

auf Seite 17

Zum Geleit

Kampf um die Cloud: Kosten kontra Funktionalität

Amazon, Google und Microsoft befinden sich am Anfang eines Preiskampfes um die Cloud. Google hatte diesen Kampf mit einer erheblichen Reduktion der Preise für seinen Cloudspeicher gestartet und Amazon hat nachgezogen. Dabei werden die neuen Amazon-Preise die Preise vieler Produkte nach unten ziehen, da Amazon die Basis für eine ganze Reihe von Produkten ist. Die Logik hinter diesen Preis-Senkungen ist klar: wer jetzt die Kunden gewinnt, kann sie behalten und hat auf Dauer einen Wettbewerbsvorteil. Amazon baut auf dieser Logik seit Jahren sein gesamtes Geschäftsmodell auf.

Was bedeutet diese Entwicklung für Unternehmens-Kunden? Um es direkt auf den Punkt zu bringen, stehen zwei Fragen im Vordergrund:

- Ein Preiskampf in der Public Cloud bringt die Nutzung von Private Cloud-Diensten unter Druck. Public Cloud Lösungen basieren mehr und mehr auf Technologien und Produkten, die dem normalen Unternehmen nicht zur Verfügung stehen (wer lässt schon seine Server nach eigenen Blaupausen in China bauen und wer verfügt schon über seine eigene Cloud-Management-Software). War ein möglicher Preisvorteil der Public Cloud noch gering, weil auch den Unternehmen Technologien wie Virtualisierung zur Verfügung standen, so ist klar absehbar, dass der Vorteil der Public Cloud wachsen wird. Unternehmen müssen zwingend auf dem neuesten Stand von Virtualisierung, Automatisierung und Cloud Management sein, um mit ihrer Private Cloud hier konkurrieren zu können. Dies betrifft sowohl Invest- als auch Betriebskosten. Speziell im Bereich der Betriebskosten sind Public Cloud-Lösungen auf einen optimalen und hochskalierbaren Betrieb optimiert.

- Unternehmen brauchen eine klare Cloud-Strategie. Die in der Public Cloud angebotenen Leistungen sind zu verschieden und die Strategien der Anbieter gehen so sehr in unterschiedliche Richtungen, dass die Auswahl einer Lösung und eines Anbieters wohl überlegt sein müssen. In jedem Fall werden nur wenige Unternehmen komplett auf Public Cloud-Lösungen umschwenken, zu viele Anwendungsbereiche lassen sich sinnvoll weiterhin nur lokal betreiben. Es wird also in jedem Fall eine gemischte Infrastruktur entstehen, die ein wohl überlegtes Konzept vor allem für den Betrieb erfordert.

Bevor wir zu der Frage der Strategie kommen, noch eine Anmerkung zur Public Cloud zu Zeiten der NSA: ist es überhaupt vertretbar, dass Unternehmen unter dem Aspekt der Sicherheit ihrer Daten Cloud-Leistungen nutzen? Dazu gibt es mehrere sich widersprechende Antworten:

- Grundsätzlich sollte ein Unternehmen die Kontrolle über seine Daten behalten und sich nicht in eine völlige Abhängigkeit von einem externen Anbieter begeben.

- Grundsätzlich gilt es, bekannten Gefahren auszuweichen und nicht bewusst die Tür für externe zu öffnen.

- Die Nutzung mobiler Endgeräte ist ohne Cloud-Dienste kaum möglich. Auch die Nutzung traditioneller Dienste wie Email setzt ja auf öffentliche Infrastrukturen. Für ein Unternehmen entsteht damit in jedem Fall die Frage der Sicherheit der eigenen Daten. Es wäre sehr naiv zu glauben, dass durch den Verzicht der Nutzung von Cloud-Diensten pauschal ein Sicherheitsvorteil entsteht und eine Abgrenzung von öffentlichen Infrastrukturen möglich ist.

- Cloud-Angebote sind nicht zuverlässig. Es gibt immer nur eine Version der angebotenen Leistung für alle. Kommt eine neue Version, kann es durchaus sein, dass Leistungsmerkmale wegfallen. So gibt es markante Beispiele dafür, dass man eine zu große Abhängigkeit von Cloud-Produkten vermeiden sollte: die Diskussion um das Ende von Google+, die Einstellung des Google Readers, der Wegfall der Diskussions-Foren bei Box, die sehr lange Diskussion um die Verfügbarkeit von Sub-Folder-Syncing bei Box und die Nichteinhaltung von Zusagen von Box über mehrere Jahre hinweg, Tücken in der Implementierung von Office 365.

- Die Sicherheit der Daten eines Unternehmens hängt nicht nur an der Cloud sondern generell an den eingesetzten Technologien und der Art ihrer Nutzung. Lücken in der Implementierung von Sicherheitsdiensten (SSL) und Browsern (siehe aktuelle Diskussion zum Internet Explorer, wieder einmal) verursachen einen deutlich größeren Schaden als das durch Cloud-Dienste passieren könnte. Und was ist wohl sicherer: die Übertragung kritischer Daten als Email-Anhänge auf ungesicherten Übertragungsstrecken oder die Nutzung eines Cloud-File-Services wie Box oder OneDrive?

- Cloud-Anbieter lernen dazu. So wird es innerhalb der nächsten 24 Monate ein klar abgegrenztes europäisches Angebot von Lösungen geben, die nicht dem amerikanischen Einfluss unterliegen sondern rein der europäischen Gesetzgebung. Auch Microsoft unterstreicht mit diversen Zertifizierungen, dass seine Server-Leistungen in Europa sicher sind (eine Frage der Glaubwürdigkeit). Aber wie immer man dies auch im Falle Microsofts sieht, die Rolle dieser Zertifizierungen wird in Zukunft sehr groß werden. Ein Einzelunternehmen ist nicht in der Lage, wirtschaftlich die Sicherheit eines Cloud-Anbieters zu prüfen (und die meisten Cloud-Anbieter lassen weder individuelle Verträge noch Prüfungen zu). Wir sprechen hier über Monster-Rechenzentren mit sehr individuellen Infrastrukturen, die sich einer normalen schnellen Überprüfung technisch vollständig entziehen. Zertifizierungen werden zu einem extrem strategischen Element werden und auch die Basis für eine juristische Akzeptanz im Einklang mit der europäischen Rechtsprechung legen.

- Gerade für kleinere Unternehmen ist der Grad an Sicherheit, der für sie wirtschaftlich mit einer eigenen Infrastruktur erreichbar ist, durchaus begrenzt. Auch wenn man pauschal der Public Cloud ein Sicherheitsrisiko unterstellt, muss man doch auch feststellen, dass das Risiko innerhalb vieler Unternehmen deutlich größer sein wird, speziell wenn es um einen gezielten Angriff auf die Daten geht.

Kampf um die Cloud: Kosten kontra Funktionalität

Ohne das weiter vertiefen zu wollen, soll an dieser Stelle deshalb ein klares Zwischenfazit gezogen werden: Unternehmen kommen an der Nutzung von Public Cloud Diensten nicht vorbei. Pauschale Sicherheitsbedenken reichen hier nicht aus, um eine solche Nutzung auszuschließen. Aber eine Nutzung von Public Cloud-Diensten ohne eine klare und wohlüberlegte Cloud-Strategie ist ohne Frage fahrlässig. Auch müssen Cloud-Anbieter und Produkte nach einem Unternehmens-spezifischen Kriterien-Katalog sorgfältig ausgewählt werden. Zum einen, um Sicherheitsbedenken gerecht zu werden, aber zum anderen auch, um sich nicht in eine langjährige Abhängigkeit vom falschen Produkt zu begeben.

Damit sind wir bei der Frage was denn Bestandteil einer Cloud-Strategie sein sollte. Dies ist ein Geleitwort und kein Technologie-Report. Deshalb sollen an dieser Stelle nur ausgewählte Elemente einer solchen Cloud-Strategie ohne Anspruch auf Vollständigkeit vorgestellt werden:

- Das Dienst-Portfolio. Hier geht es im Kern um die Entscheidung Best-of-Breed kontra Integrierte Funktionalität (wie so oft in der Geschichte der IT). Cloud-Speicherdienste ohne Zusatzfunktionalität sind auf Dauer eine Sackgasse. Dropbox geht momentan den Weg, solche Dienste selber als Value-added anzubieten. Box hat den Weg über offene APIs und Kooperationen mit Unternehmen wie Jive oder Smartsheet gewählt. Microsoft stellt demgegenüber ein umfangreiches Gesamtportfolio aus eigenen Cloud-Produkten bereit. Ein Unternehmen sollte mindestens neben den Speicherdiensten Dienste aus dem Bereich Diskussionsforen und Task-Management erwägen. In jedem Fall sollte unterstellt werden, dass ein einzelner Anbieter nicht in der Lage sein wird, alle Anforderungen zu erfüllen. Die Offenheit einer Lösung und der Umfang der Kooperation mit anderen Cloud-Software-Anbietern spielt also eine große Rolle. Zum Beispiel deckt Microsoft mit seinem Office 365 und Azure sicher viele Bereiche ab. Aber nicht alle diese Bereiche sind überzeugend. Yammer ist ein sehr gutes und intuitives Tool. Aber für größere Unternehmen und Service-Organisationen kann die Anpassbarkeit eines Produktes wie Jive von zentraler Bedeutung sein. Auch im Bereich Task-Management gibt es viele gute und spezialisierte Produkte, die ggf. besser zum Unternehmen passen. Generell sollte ein Gesamtgebilde entstehen, das verschiedene Versionen desselben Dokuments vermeidet. Also kein Transfer per Email, keine Kopie eines Dokuments in einem Diskussionsforum oder einer Taskliste.

- Integration mit Lokalen Geräten, Technologien und Infrastrukturen (klare Auflistung: wer, was, wie, wann, wo). Ein gutes Beispiel hierfür ist die Synchronisation von Dateien zwischen der Cloud und lokalen Endgeräten. Dropbox hat diese Synchronisation groß gemacht, aber mehrere andere Anbieter unter spezieller Nennung von Box und Huddle haben erfolgreich gezeigt, wie eine solche Synchronisation auch Probleme bereiten kann. Solche Integrations-Merkmale müssen klar und auch im Detail festgelegt werden. Die Produktauswahl wird dadurch wesentlich bestimmt.

- Die Integration von Externen und die Überwachung dieser Integration.

- Die Sicherheit des Dienstangebots.

- Die Abgrenzung zwischen Private und Public Cloud.

- Ein Betriebskonzept. Wer ist zuständig und wie sind die Abläufe, wenn etwas nicht funktioniert. Wie kann der Betrieb überwacht werden, welche Schnittstellen bietet der Cloud-Anbieter für ein SLA-Management.

- Die Auflistung notwendiger Zertifizierungen des Cloud-Anbieters.

- Eine Einschränkung möglicher Server-Standorte von Anbietern unter Berücksichtigung der dafür zuständigen Gesetzgebungen.

- Ein integriertes Sicherheitskonzept, das sowohl die Cloud als auch die betroffenen Endgeräte mit den lokalen Infrastrukturen als auch die Benutzer umfasst.

An dieser kleinen Liste ist bereits leicht zu erkennen, dass die Entwicklung einer Cloud-Strategie nicht trivial ist. Hier kommen komplexe technische Elemente mit organisatorischen Elementen und einer Kostenbetrachtung zusammen. Gleichzeitig wird hier ein Fundament gelegt, das in den meisten Fällen ja mehrere Jahre halten soll, es muss also in sich plausibel und stabil sein.

Also zum Abschluss noch einmal die beiden Kernpunkte als Fazit:

- Bei allen Bedenken und Abwägungen: an Public Cloud-Lösungen wird auf Dauer kein Unternehmen und keine Behörde vorbei kommen.

- Dies erfordert eine klare und auf langjährige Nutzung ausgelegte Cloud-Strategie, ein Fundament, das sowohl Sicherheit als auch Funktionalität gewährleisten soll.

Die Cloud ist da. Auch wenn wir von ComConsult Research nach wie vor Zweifel an dem Sinn bestimmter Cloud-Leistungen haben (IaaS speziell), so sind Cloud-Dienste im Sinne erweiterter SaaS-Angebote schlicht unverzichtbar. Ich komme auf ein entscheidendes Beispiel zurück: die Übertragung sensitiver Dokumente per Email ist um Dimensionen unsicherer und fragwürdiger als die Speicherung desselben Dokuments in einem Cloud-Dienst. Es bleibt nur eine sinnvolle Schlussfolgerung übrig: eine Unternehmensspezifische Cloud-Strategie muss geschaffen werden, die das benötigte Fundament für die nächsten Jahre legt.

Ihr
Dr. Jürgen Suppan

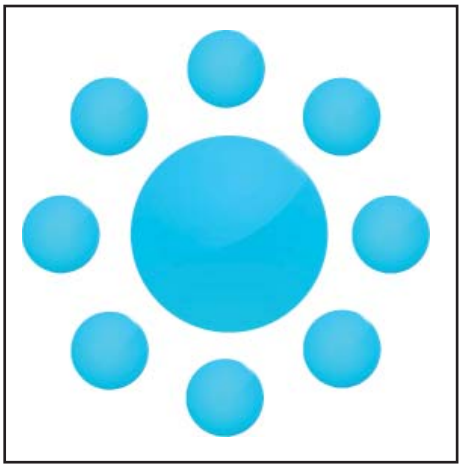
Intensiv-Update auf den neuesten Stand der Netzwerktechnik

ComConsult Sommerschule 2014

30.06. - 04.07.14 in Aachen

Die ComConsult Akademie veranstaltet vom 30.06. bis 04.07.14 ihr "ComConsult Sommerschule 2014" in Aachen.

Netzwerke unterliegen einer permanenten Weiterentwicklung. 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. Neue Standards zur Gestaltung von Netzwerken im Rechenzentrum und im Backbone sind gute Beispiele dafür. Zukunftsorientiertes und wirtschaftlich optimales Design muss dieses Gesamtbild berücksichtigen. Die ComConsult Sommerschule 2014 analysiert und diskutiert diese Änderungen und ihre Auswirkungen speziell auf die Netzwerk-Infrastrukturen. Top Experten haben das Programm der Sommerschule gestaltet und systematisch die Erfahrungen laufender Projekte und neuester Technologie-Entwicklungen eingearbeitet. Treffen Sie einige der besten Experten, die die deutsche Netzwerk-Landschaft zu bieten hat.



Frühbucherphase bis 31.05.14
Sparen Sie 200,- €

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Sommerschule 2014 - Intensiv-Update auf den neuesten Stand der Netzwerktechnik

Ich buche das Seminar
Sommerschule 2014

☐ vom 30.06. - 04.07.14 in Aachen
zum Preis € 2.290,-- netto*
*gültig bis zum 31.05.14

Bitte reservieren Sie mir ein Zimmer

vom _____ bis _____ 14

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

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

Programmübersicht Sommerschule 2014

Montag, der 30.06.14 - IT-Architekturen und Auswirkungen auf Netzwerke

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. Ohne Zweifel wird unsere IT-Landschaft in fünf 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.

9:30 - 17:00 Uhr
Wir analysieren für Sie:
- Wie ändert sich IT und welche Auswirkungen hat das auf Infrastrukturen?
- Was passiert auf der Netzwerk-Seite, um diesen Anforderungen zu entsprechen?
- Welche neuen Technologien müssen speziell bei den Planungen für die nächsten Jahre beachtet werden?
- Was muss speziell im WAN passieren, um den neuen Anforderungen zu entsprechen, wie ist der Status im WAN und welche Optionen bestehen?
- Welche Herausforderungen und Technologien bringt das Internet of Things in bestehende IT-Architekturen?

Dr. Franz-Joachim Kauffels,
unabhängiger Technologie- und Industrie-Analyst
Dr.-Ing. Behrooz Moayeri,
ComConsult Beratung und Planung 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 01.07.14 - LAN-Technologien: aktuelle Entwicklungen

LAN-Technik wird im Moment neu erfunden. Neue Anforderungen erfordern neue Lösungen. Programmierbare Netzwerke als Teil des Software Defined Data Center und als Teil von Software Defined Infrastrukturen sind ein Beispiel dafür. Neue Fabric-Konzepte, ein Umdenken bei VLAN-Technik, eine Neupositionierung von QoS und neue Nutzungsformen im Rahmen von Audio-/Video-Bridging sind herausragende Beispiele. Wir erklären, was im Moment passiert und wie Sie sich auf die Zukunft vorbereiten.

9:00 - 17:00 Uhr
Sie lernen in diesem Themenblock:
- Welche neuen LAN-Technologien gibt es, welche Konsequenzen hat das?
- Netzwerk-Design mit 10/40/100 Gigabit, wie sehen Anforderungen und Plaungs-Ansätze aus?
- Fabric-Konzepte verdrängen traditionelle Architekturen: was leisten sie und wie können sie sinnvoll eingesetzt werden?
- Quo Vadis VLAN-Technik: werden VLANs durch Edge-Provisioning und Overlays verdrängt?

Dipl.-Inform. Petra Borwoka-Gatzweiler,
Planungsbüro UBN

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

Mittwoch, der 02.07.14 - Sicherheit / Unified Communications: wo stehen wir?

Sicherheit in der IT wird zum dominierenden Thema der nächsten Jahre. Aber hier geht es nicht um hochfliegende Träume sondern um ein solides Fundament aus Basis-Sicherheits-Funktionen.

9:00 - 12:30 Uhr
Dies ist das Thema des Bereichs Sicherheit in der Sommerschule:
- Sicherheit im LAN: neueste Entwicklungen
- Sicherheit und mobile Endgeräte: haben wir noch eine Chance unsere Sicherheit zu retten?
- Sicherheit und UC: immer offener und immer sicherer, ist das ein unlösbarer Widerspruch?

Dr. Simon Hoff,
ComConsult Beratung und Planung GmbH

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.

14:00 - 17:00 Uhr
In diesem Block lernen Sie:
- Wo steht UC heute?
- Was leisten wichtige Produkte?
- Wie sieht die Zukunft des Clients aus?
- Wird das Telefon als Endgerät verdrängt?
- Neue Video-Standards: wo geht der Weg hin?

Dipl.-Inform. Petra Borwoka-Gatzweiler,
Planungsbüro UBN
Markus Geller,
ComConsult Research GmbH

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

Donnerstag, der 03.07.14 - Integration Mobiler Endgeräte / WLAN und Mobilfunk

Die Integration Mobiler Endgeräte umfasst ein weites Spektrum an Aufgaben: den Zugang, die Zuordnung eines Rechteprofils, die Erarbeitung eines Unternehmens-spezifischen App-Shops, die Bereitstellung einer Infrastruktur im Rechenzentrum. Gleichzeitig haben mobile Endgeräte breite Auswirkungen auf die Nutzung traditioneller Applikationen. So müssen UC-Lösungen angepasst werden und auch Funktionsbereiche wie Dokumenten-Verarbeitung und Management müssen neu positioniert werden.

9:00 - 12:30 Uhr
Wir analysieren in diesem Block
- Wie die neue Mitarbeiter-Mobilität die Unternehmens-IT beeinflusst
- Welche mobilen Plattformen für das Unternehmen relevant sind
- Welche Beschaffungs- und Betriebskonzepte zu unterscheiden sind
- Wie man den sicheren Zugriff auf Applikationen ermöglicht
- Was ein Mobile Device Management für die IT leisten kann
- Welche Auswirkungen Mobile Computing auf das Netz hat
- Was sich hinter Multi Path TCP (MPTCP) verbirgt
- Welche Anforderungen eine „Mobile Readiness“ beinhaltet

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

Mit der rasanten Zunahme mobiler Endgeräte bekommt der Zugang dieser Geräte zu den Unternehmens-Infrastrukturen eine zentrale Bedeutung. In Zukunft werden deutlich mehr Endgeräte diesen Zugang wählen als die Kabel-basierte Alternative. Denkt man einen Schritt weiter zum Internet of Everything, dann wird die zukünftige strategische Bedeutung des Zugangs über WLAN und Mobilfunk deutlich. Sowohl die schiere Anzahl der Teilnehmer als auch der damit verbundene Schutz- und Kontrollbedarf machen Änderungen an der Netzwerk-Infrastruktur erforderlich.

14:00 - 17:00 Uhr
In diesem Themenblock lernen Sie:
- Welche Optionen Ihnen das moderne WLAN bietet
- Wie sich Mobilfunk-Alternativen demgegenüber positionieren

Dr. Franz-Joachim Kauffels,
unabhängiger Technologie- und Industrie-Analyst

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

Freitag, der 04.07.14 - RZ-Technik

Rechenzentren sind von allen Seiten unter Druck:
- Die Cloud generiert einen direkten Kostenvergleich und puscht das Thema Wirtschaftlichkeit im RZ noch weiter als bisher
- Infrastrukturen für mobile Endgeräte erfordern den Aufbau einer private Cloud und setzen neue Anforderungen an Infrastrukturen
- Server- und Speicher-Konsolidierungen gehen permanent weiter, neue Perspektiven entstehen und stellen alle traditionellen Ansätze in Frage
- Virtualisierung geht in die nächste Runde, leistet noch mehr, stellt aber auch immer mehr und immer schwierigere Anforderungen an die Infrastrukturen

Angesichts dieser Entwicklungen brauchen Rechenzentren eine neue und Zukunfts-orientierte Infrastruktur-Strategie.

9:00 - 15:30 Uhr
Sie lernen in diesem Themenblock:
- Was passiert im RZ, welche neuen Anforderungen entstehen?
- Wo stehen Server und Speicher?
- Welche Anforderungen generiert Virtualisierung?
- Dienstneutralität im Netzwerk: geht das noch im RZ der Zukunft? Brauchen wir ein neues Verständnis von Netzwerken?
- Open Stack und SDN: das Fundament für das Software Defined Data Center, Provider-Technologien oder eine neue Chance für Unternehmen?

Dipl.-Math. Cornelius Höchel-Winter
ComConsult Research GmbH
Dr. Joachim Wetzlar,
ComConsult Beratung und Planung GmbH

10:30 - 10:45 Uhr Kaffeepause
13:00 - 14:00 Uhr Mittagspause
15:30 Uhr Ende der Veranstaltung

Schwerpunkthema

Enterprise App Stores

Fortsetzung von Seite 1

Dipl.-Inform. Dominik Franke ist Leiter des Competence Centers für Mobile Applications & IoT. Sein Fokus liegt auf der Strategie- und Prozessberatung für die Einführung mobiler und smarter Lösungen in bestehende Unternehmens-IT.

Software für mobile Endgeräte wie Smartphones, Tablets und Phablets, sogenannte „Apps“, werden heutzutage nicht über traditionelle Trägermedien übertragen, sondern über „App Stores“. Jeder Smartphone-Benutzer kennt diese App Stores und kann sie vom ersten Tag an bedienen. Kaum jemand hinterfragt diese Technik, wie sie sich so weit und still verbreiten konnte und insbesondere, was sie für ein Unternehmen mit mobilen Endgeräten bedeutet. Dieser Artikel beschäftigt sich mit der Verwendung von App Stores im Unternehmensumfeld und beleuchtet sowohl die Vor- als auch Nachteile, die eine solche Lösung mit sich bringt. Zudem werden App Store-Lösungen für den Unternehmensbereich diskutiert, sowie Auswirkungen einer Implementierung von App Stores in der Unternehmens-IT analysiert.

Und am 5. Tag erschuf Apple den App Store…

Der Begriff „App Store“ ist eine Wortkreation aus dem Englischen (Application = Anwendung, Store = Geschäft) und steht heute im mobilen Umfeld für eine Vertriebsplattform für mobile Anwendungen. Wenn man heutzutage in den Nachrichten von App Stores hört, dann ist dies eher auf Kuriositäten als auf neue Errungenschaften zurückzuführen. So schaffte es beispielsweise ein achtjähriges Mädchen in den Vereinigten Staaten durch Apps für Kinder (z.B. eine Anwendung, in der man sein eigenes Pony pflegt und ausrüstet) über 6000$ auszugeben (z.B. mit einen Diamanten-verzierten Sattel für mehrere hundert US-Dollar). App Stores werden von Benutzern unter anderem deswegen als sehr komfortable Einkaufsplattform wahrgenommen, weil man die Authentisierung und die Kontoinformationen (Kreditkartennummer, …) nicht bei jedem Kauf eingeben muss. Das Kaufen ist also in der Tat kinderleicht geworden. So kann auch eine achtjährige ohne Zuhilfenahme der Eltern sowohl Apps als auch in-App Käufe tätigen. Während App-Käufe in der App Store-Umgebung stattfinden, werden in-App Käufe innerhalb einer Anwendung getätigt (z.B. Kauf von Büchern innerhalb einer Bibliotheks-App). Die Eltern der achtjährigen haben Apple dafür verklagt, dass ihr Kind so einfach so viel Geld ohne ihr Wissen ausgeben konnte und dass die Eltern keine Möglichkeit hatten etwas dagegen zu tun. Etwas anders formuliert: Die Eltern haben also gegen die hohe Benutzerfreundlichkeit von App Stores geklagt. Und sie haben Recht bekommen. Apple hat den Eltern und in weiteren ähnlichen Fällen das Geld erstattet. Um weiteren ähnlichen Fällen vorzubeugen, hat Apple zudem einen Mechanismus eingeführt, der beispielsweise die Eingabe einer PIN vor dem Kauf jeder kostenpflichtigen App oder bei in-App Käufen erzwingt. Dieser Mechanismus eignet sich also ebenso als Kindersicherung.

Sonst sind App Stores eher unscheinbar und selbstverständlich. Sie kommen üblicherweise als separate mobile Anwendung mit dem Betriebssystem. Dies ist notwendig, da App Stores tief in das Betriebssystem eingreifen müssen. Seitens der Plattform sind sie als einziges Medium dafür gedacht, neue Anwendungen installieren und entfernen zu dürfen. Bei einer Installation werden Apps zudem Rechte eingeräumt, die man auf Betriebssystemebene einzig mit Root-Rechten erhält. Beispielsweise werden Anwendungen bei der Installation Zugriffe auf Hardwarekomponenten wie Kamera, GPS und SD-Karten zugesprochen.

App Stores sind im Grunde aufgebaut wie eine klassische Software-Abteilung im Mediamarkt oder Saturn. Abbildung 1 präsentiert den Blick auf Google’s App Store „Google Play“ wie man ihn entweder mit einem Tablet oder einem Internet-Browser sieht. Die Apps in App Stores sind nach Kategorien unterteilt. Einerseits gibt es ähnliche Kategorien wie man sie im Mediamarkt erwarten würde: Bildung (Wikipedia, Duden, …), Nachrichten (Tagesschau, Mediatheken, …), Outdoor (Geocaching, Navigationssysteme, …) etc. Andererseits gibt es Kategorien, wie man sie im Mediamarkt nicht hat: „Was Freunde kaufen“, „Für Sie empfohlen“ etc. Man erkennt also die allgegenwärtige Personalisierung des Internets als auch die Macht und Datenmenge, die hinter einem solchen App Store steckt. Neben den Kategorien gibt es für jede App eine Beschreibung. Da Menschen auf mobilen Endgeräten ungerne viel lesen, sind die Beschreibungen in der Regel recht kurz gehalten (200-1000 Zeichen anstatt ganze Handbücher). Wie bei Amazon findet man auch in App Stores zu jeder App eine Bewertung der Benutzer, die die App bereits installiert und ausprobiert haben. So gibt es beispielsweise eine Skala mit einer 5-Sterne-Bewertung als auch die Anzahl der Downloads für diese App. Letzteres hilft den Kunden von öffentlichen App Stores beispielsweise bekannte und etablierte Apps von möglicher Malware zu unterscheiden. So kann eine Top-Bewertung bei weniger als 100 Downloads eher auf Malware hindeuten als über 100 Mio. Downloads bei einer Bewertung von vier (von fünf) Sternen. Und eines ist sicher: Bei über einer Million Apps in den großen öffentlichen App Stores muss man sich vor Malware und Viren in Acht nehmen.

Apps spielen in App Stores ohne Zweifel die wichtigste Rolle. Jedoch können App Stores heutzutage auch wesentlich mehr. So gibt es beispielsweise App Stores, welche auch Musik, Videos, Handbücher, E-Books, Skins, Themes, Plugins etc. vertreiben können. In einem Un-

Enterprise App Stores

ternehmen ist ein solcher Vertriebsweg für Dokumente und Handbücher durchaus hilfreich. Neben kostenfreien gibt es in einem App Store auch kostenpflichtige Apps. Die Kaufabwicklung übernimmt der App Store. Kontoinformationen (z.B. Kreditkarteninformationen) muss man dabei entweder bei der ersten Verwendung der App Store App oder beim Kauf einer ersten kostenpflichtigen App eingeben. Neben der Kaufabwicklung übernimmt die App Store App auf mobilen Endgeräten auch die Installation. Nach der Auswahl einer entsprechenden App im Store kann der Benutzer die Installation mit einem einzigen Klick einleiten. Im ersten Schritt werden ihm sämtliche Rechte angezeigt, welche die App für sich beansprucht. Hierzu gehören beispielsweise: „Zugriff auf Bluetooth“, „Verschicken von SMS“ und „Nummern ohne Benachrichtigung wählen“. Wenn beispielsweise eine Spiele-App wie Angry Birds Zugriff auf die gesamte Kontaktliste haben möchte, so ist bereits Vorsicht geboten. So wurde im Rahmen der NSA-Leaks auch bekannt, dass die NSA tatsächlich die von der Angry Birds App abgegriffenen Daten (u.a. Kontaktdaten der Nutzer) erhalten hat (auf welchem Wege auch immer). Ein solches Szenario ist in einem Unternehmensumfeld selbstverständlich völlig obsolet, aber durch den Zugriff auf öffentliche App Stores von Geräten mit unternehmenssensiblen Informationen auf keinen Fall unrealistisch. Die Absicherung des App Stores oder die Verwendung einer entsprechenden Enterprise App Store-Lösung kann eine solche Gefahr minimieren. Ein häufiger Workaround ist beispielsweise die Unterbindung von unerlaubten oder unbekannten Anwendungen auf Netzwerkebene (z.B. Sperrung bestimmter Ports). Sobald der Benutzer jedoch beispielsweise eine mobile Datenverbindung aufbaut oder sich im heimischen WLAN verbindet, sendet die App eben dann die abgegriffenen und sensiblen Daten an ihre Entwickler. Im zweiten Schritt der Installation wird die mobile Anwendung auf dem Endgerät installiert. Das geschieht ohne Interaktion mit dem Benutzer. Während bei typischen Installationen auf Desktop-Systemen der Benutzer beispielsweise den Pfad oder unterschiedliche Parameter einer Installation beeinflussen kann, besteht die Möglichkeit bei der Installation einer App auf einem mobilen Endgerät nicht. Für den Benutzer ist der Vorteil dabei, dass er sich um Parameter und Pfade keine Gedanken machen muss. Für den technischen Verantwortlichen ist der Vorteil, dass Benutzer zumindest bei der Installation nichts falsch machen und die einfache Installation auch ohne sein Mitwirken bewerkstelligen können. Im abschließenden Schritt einer Installation werden Verknüpfungen im Hauptmenü sowie auf dem Startbildschirm des Gerätes angelegt. Neben Installationen bieten App Stores auch noch die Möglichkeit Updates zu vertreiben. Bei einem Desktop-System hat man grundsätzlich drei Möglichkeiten Softwareupdates zu erhalten. Entweder es läuft ein separater Service im Hintergrund, der regelmäßig selbst nach Updates sucht (z.B. Java- oder Windows-Updater) oder die Anwendung selbst überprüft bei jedem Start ihren Updatestatus, oder der Benutzer startet den Update-Prozess manuell. Der Vorteil eines App Stores als zentrale Vertriebsstelle für Apps ist die Möglichkeit alle Benutzer, die eine bestimmte App installiert haben, unmittelbar über ein erhältliches Update zu informieren und dieses entweder automatisch oder mit einem Klick zu installieren. So können Sicherheitsupdates für alle Apps, die der Benutzer auf seinem Smartphone hat, stets schnell und zeitnah vertrieben werden.

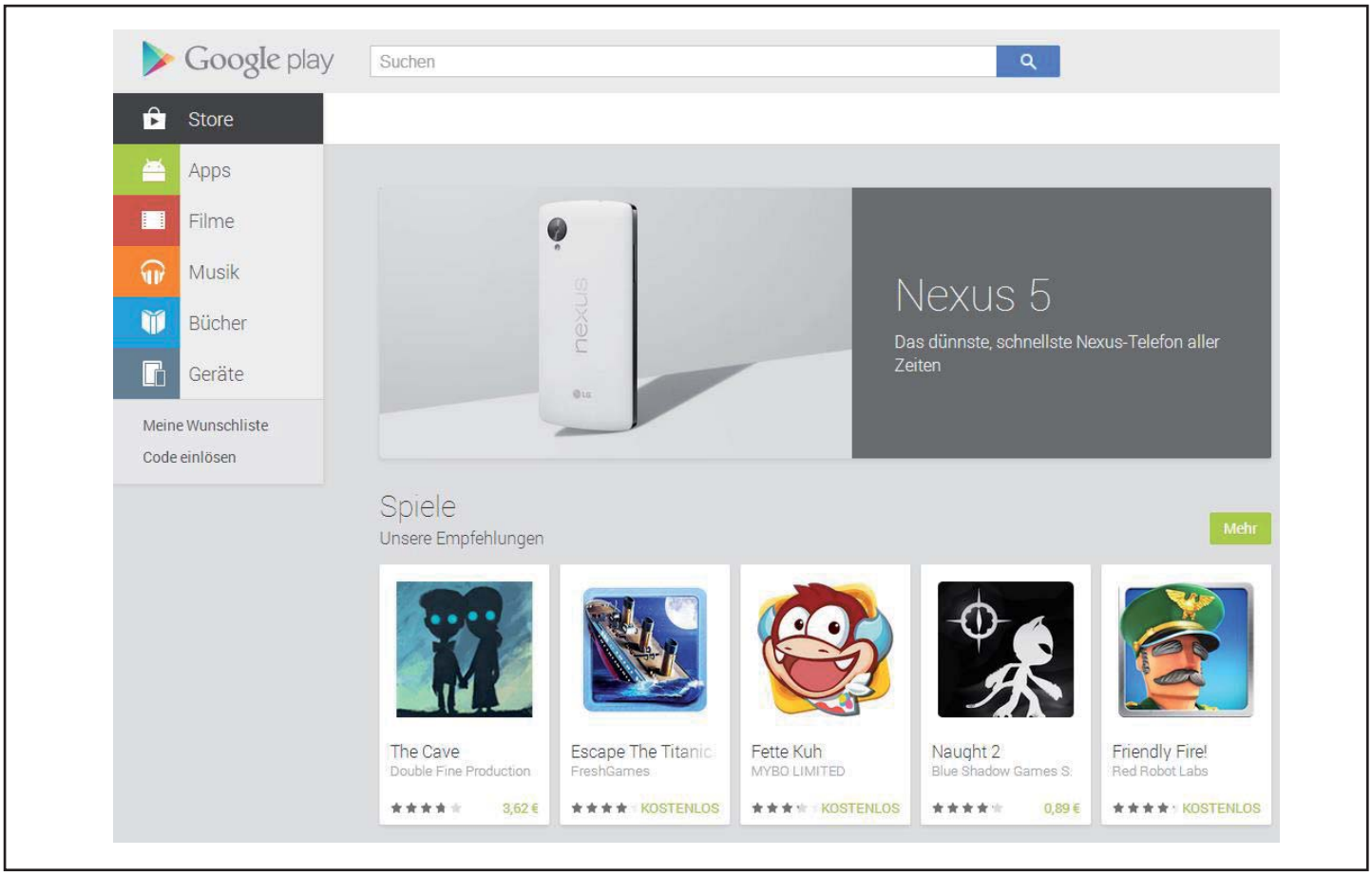


Abbildung 1: Blick in den App Store Google Play

Quelle: Google Play App Store

Enterprise App Stores

App Stores sind nicht neu

App Stores gibt es in der Tat schon eine ganze Weile und in zahlreichen unterschiedlichen Gewändern. Bereits 1993 gab es den Electronic AppWrapper für das Betriebssystem NEXTSTEP von NEXT. Zu der Zeit konnte man Apps noch über Telefon und E-Mail ordern. 1994 haben sich Linux-Systeme wie pkgsrc und APT verbreitet, die durchaus bis heute beispielsweise auf Linux-Servern Standard sind. Sie bieten die Möglichkeit ohne eine GUI Pakete herunterzuladen und automatisch zu extrahieren. BeDepot des Betriebssystems BeOS war der erste App Store, der sowohl kostenlose als auch kostenpflichtige Anwendungen angeboten hat und eine Update-Funktion hatte. Handango (2003) war der erste App Store, welcher Apps für mobile Endgeräte angeboten hat. Ein weiterer Pionier war der Nokia 770 Internet Tablet App Store aus dem Jahr 2005. 2007 erschien das erste iPhone. Dieses hat den Benutzern jedoch nur die Software zur Verfügung gestellt, die bereits auf dem Gerät vorinstalliert war. Bei ihrem Streben um Individualismus hat die iPhone Community jedoch schnell einen Jailbreak für das iPhone gefunden (= Beschaffen von Root-Rechten) und konnte anschließend Software von Drittanbietern auf den Geräten installieren. Dieser Markt florierte so schnell und stark, dass Apple knapp 1 Jahr nach dem Release des ersten iPhone den App Store für das iPhone einführte (Juli 2008). Damit war der Grundstein für das, was wir heute als selbstverständlich bei Smartphones erachten, gelegt. Dieser Entwicklung folgten schnell die Kontrahenten: Googles Play Store (September 2008), Blackberry World (April 2009), Windows Phone Store (Oktober 2010), Mac App Store (Januar 2011), Amazons App-Shop (März 2011) und Windows Store (Februar 2012).

Apple's App Store war de facto der erste App Store für die heutige Smartphone-Generation und bietet bereits über 1 Mio. Apps (Stand Oktober 2013). Der Hauptbeschaffungsweg für Apps ist die App Store App, welche auf den Geräten iPhone, iPad und iPod-Touch zur Verfügung steht. Im Store gibt es sowohl kostenlose als auch kostenpflichtige Apps. Kostenpflichtige Apps kosten ein Vielfaches von einem Dollar minus 1 Cent (z.B. 1,99$). Apple behält 30% aller Umsätze die von einer App generiert werden (sowohl durch den App-Kauf als auch durch in-App Käufe). Diese Marge gilt auch für Googles Play Store, welche ebenfalls über 1 Mio. Apps anbietet (Juli 2013). Die Apps dürfen bei Google bis zu 4,05 GB groß sein. Neben der Google Play App gibt es bei Google auch die Möglichkeit Anwendungen remote über ein Webinterface auf Geräten zu installieren. Die gleichen Möglichkeiten bietet Microsofts Windows Phone Store mit über 200.000 Apps (Dezember 2013). Microsofts Windows Store bietet über 140.000 Apps für die Oberfläche Modern UI an. Diese Oberfläche findet man sowohl bei Windows 8 als auch bei Windows Phone Geräten. Microsoft versucht hier durch die Ausrichtung von Windows 8 auf Convertibles und Tablets Synergien zwischen den beiden Betriebssystemen Windows Phone und Windows 8 zu schaffen. Dadurch wird eine Portierung von Windows Phone Apps auf Windows 8 wesentlich erleichtert und das Look-and-Feel bleibt ähnlich. Blackberry World hält über 120.000 Anwendungen (September 2013), jedoch mit einer stark durchwachsenen Qualität, und Amazons App-Shop über 75.000 Apps. Amazons App-Shop bietet die Anwendungen für mobile Endgeräte von Amazon wie das Kindle Fire HD an. Diese Geräte laufen ebenfalls mit Android (wie die Google-Geräte), haben jedoch ein angepasstes Amazon Frontend. Somit bietet Amazons App-Shop genau wie Google Play Android-Apps an. Jedoch muss hier beachtet werden, dass eine gekaufte App bei Google Play nicht zugleich beim Amazon App-Shop für den gleichen Benutzer verfügbar ist. Da die beiden Stores getrennt sind, muss die gleiche App in beiden Stores separat gekauft werden um diese auf zwei Geräten mit den beiden Plattformen verfügbar zu haben.

Hardware über App Stores beziehen

Die Bekanntheit von App Stores rührt insbesondere aus dem Software-Umfeld bei mobilen Endgeräten. Zu Vertretern dieser Art von App Stores gehört der Großteil der bereits genannten Stores. Es gibt jedoch auch immer mehr App Stores, welche Software für den Desktop-Bereich anbieten. Hierzu gehören die bereits genannten Stores Windows Store und Mac App Store. Weitere Vertreter dieser Gruppe sind Steam, Firefox Marketplace und Chrome Web Store. Die beiden letztgenannten bieten kostenlose und kostenpflichtige Apps für die Browser Firefox und Chrome an. Insbesondere bedienen sie aber auch die entsprechenden Betriebssysteme Firefox OS und Chrome OS, welche als Kernkomponente den jeweiligen Browser anbieten. Google geht

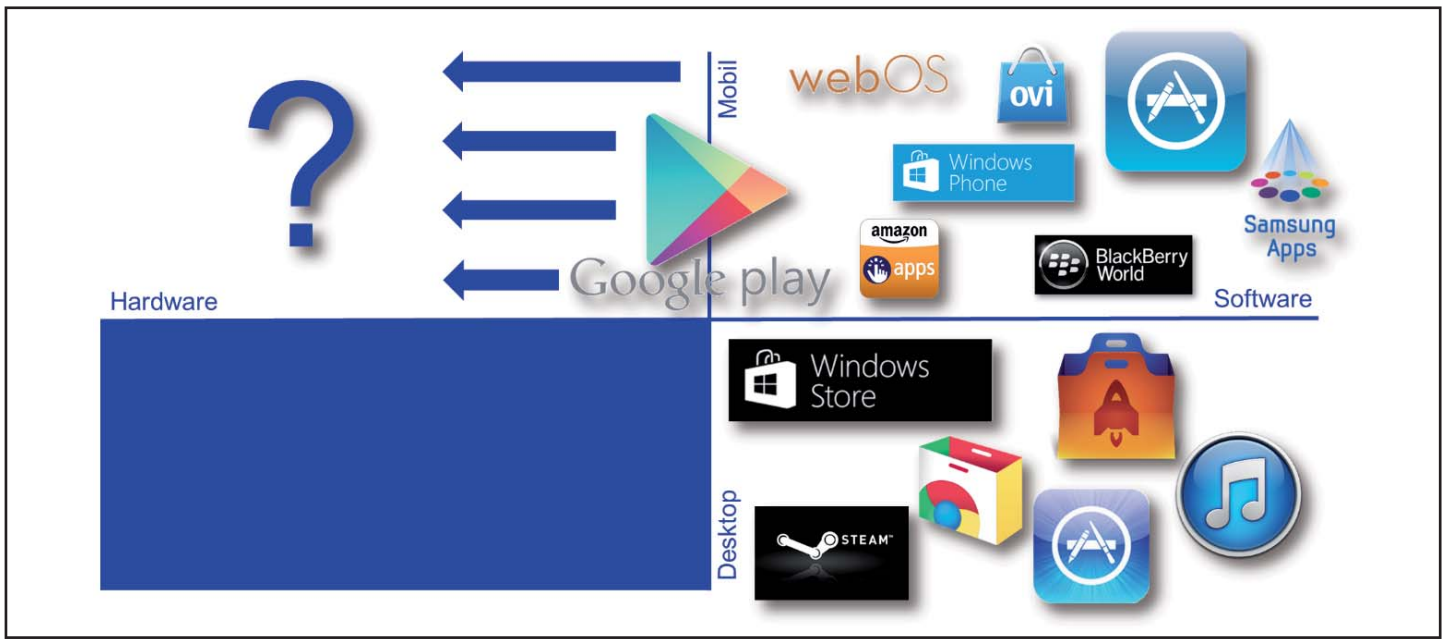


Abbildung 2: App Store Trends

mit seinem Google Play Store allerdings noch einen Schritt weiter und bietet über diesen auch Hardware an (siehe Abbildung 2). Hierzu gehören sämtliche Nexus-Geräte, passende Accessoires, Chromecast-Sticks und künftig auch Google Glass. Der Vorteil für den Benutzer ist, dass er mit einem einfachen Klick ein neues Smartphone für mehrere Hundert Euro kaufen kann – genauso einfach wie eine App. Die Bestellung geht an Google und die Ware wird unmittelbar von der jeweiligen Produktions- oder Vertriebsstätte (z.B. China) an die Person versandt. Die Vorteile für Google sind dabei nicht zu unterschätzen. Google hat bei den Smartphones zurzeit über 76% Marktanteil (Stand 4Q2013) und all diese Geräte haben Android und Google Play installiert. Mit einem Klick können alle Benutzer Hardware im Wert von mehreren Hundert Euro kaufen. Google erfährt dadurch keine gesonderten Vertriebs- oder Marketingkosten, da Google Play bereits existiert, funktioniert und auf allen Geräten verfügbar ist. Ob die anderen Stores in die gleiche Richtung ziehen werden, ist abzuwarten. Es ist nun einmal auch eine Tatsache, dass das Einkaufserlebnis in einem begehbaren und hochwertigen Apple Store sich wesentlich von dem in einer Google Play App unterscheidet.

Weitere App-Store Trends, die sich abzeichnen:

- Es werden weniger Umsätze mit Apps erzielt, dafür mehr mit in-App Käufen.

- Android Apps laufen auf immer mehr unterschiedlichen Plattformen (wie Amazons Kindle Fire HD, Blackberry Geräte, …), sodass auch Android Apps nicht nur im ursprünglichen Google Play Store verfügbar sind.

- Es zeichnet sich ein Trend in Richtung HTML5 in Kombination mit nativen Anwendungen ab. Die Vorteile sind die erhöhte Plattformunabhängigkeit und nur noch eine einzige zu pflegende Codebasis, was Entwicklungskosten wesentlich reduzieren kann. Somit sind vermehrt Apps in Stores zu erwarten, die eine native Hülle als Laufzeitumgebung für HTML5 Content anbieten, der anschließend entweder nachgeladen wird oder den die App selbst mitbringt.

- Aufgrund von viel Malware und einer geringen Qualität vieler Apps in den großen App Stores, arbeiten die App Store Betreiber an einer Sicherstellung eines zufriedenstellenden Qualitätsstandards der Apps. Es ist also davon auszugehen, dass zukünftig die Qualität statt Quantität der Apps im Vordergrund stehen wird.

- Aufgrund der üblicherweise geringen Preise für Apps in App Stores (verglichen mit Preisen für Desktop-Software) geht der Trend bei den Entwicklern zum Splitten großer Softwarepakete in mehrere kleine Pakete. Beispiel: Microsoft Office kauft man nicht als Gesamtpaket, sondern die einzelnen Anwendungen (Word, Excel, …) separat zu einem entsprechend geringeren Preis.

Plattformunabhängige App Stores

Neben den hier erwähnten App Stores, welche in der Regel an die jeweilige Plattform angebunden sind, gibt es auch plattformunabhängige App Stores, wie zum Beispiel GetJar, Appitalism und Apperia. Durch ihre Plattformunabhängigkeit können solche Stores sowohl Android als auch iOS Apps anbieten. Zudem werden hier Apps angeboten, die in die offiziellen App Stores nicht aufgenommen wurden (z.B. Absage aufgrund von Malware-Verdacht). Apps, die in einen solchen Store aufgenommen werden, müssen den Vorgaben der offiziellen Stores nicht nachkommen (z.B. Vorgaben zum Design oder zur Performance-Sicherstellung). Diese Art der Stores blüht daher insbesondere in Ländern auf, die keinen oder nur sehr eingeschränkten Zugang zu den offiziellen Stores haben (z.B. China). Ein unmittelbarer Nachteil eines solchen inoffiziellen Stores ist jedoch ein wesentlich höherer Anteil an Malware und Viren. Es ist häufig unklar, wer hinter den Stores sitzt, wer die Apps zertifiziert und wie die Prozesse zur Qualitätssicherstellung (z.B. durch statische Analyse, Beta-Testing wie bei Apple oder den Google Bouncer) aussehen. Als Unternehmen kann man einem solchen Store daher kaum trauen. So könnte beispielsweise eine unternehmenseigene App nach dem Hochladen in den Store modifiziert (z.B. infiziert) und dennoch durch den Store-Betreiber mit einem echten Zertifikat versehen werden. Die hochgeladene App würde dann nicht mehr der anschließend herunterladbaren App entsprechen. Zudem könnten weitere Apps mit dem gleichen Zertifikat signiert und veröffentlicht werden, was den Eindruck erweckt, es seien eigene Apps, denen die Mitarbeiter blind vertrauen könnten.

Zwei Seiten der Medaille

App Stores bieten in Unternehmen diverse Vorteile, aber auch Nachteile für Mitarbeiter und das Unternehmen.

Vorteile für Mitarbeiter:

- Benutzerfreundlichkeit: App Stores sind als App leicht zu bedienen und zu durchstöbern. Die bekannte Handhabung mit CDs, Lizenzschlüsseln und Installationsanleitungen entfällt.

- Einzige Anlaufstelle: Alle Apps werden zentral an einer Stelle angeboten. Das Suchen auf Netzlaufwerken und die Telefonate mit Admins entfallen.

- Installation & Updates: Diese werden entweder automatisch oder mit wenigen Klicks vom App Store übernommen. Im App Store gibt es stets die aktuellste Version, sodass man nicht mit unterschiedlichen CDs und Versionen der Software umgehen muss.

Vorteile für das Unternehmen:

- Zentrale Verwaltung von Updates: Durch die zentrale Update-Verwaltung mit Benachrichtigung der Mitarbeiter kann dafür gesorgt werden, dass sicherheitskritische Updates schnell an alle Mitarbeiter kommen. Mit einer entsprechenden Mobile Device Management (MDM) Lösung können Updates zudem erzwungen werden.

- Time to Market: Vom Unternehmen in Auftrag gegebene Custom Apps müssen nicht erst auf CD gedruckt und dann traditionell an alle Mitarbeiter verteilt werden. Software muss auch nicht auf ein Netzlaufwerk abgelegt werden und anschließend alle betroffenen Mitarbeiter über E-Mail informiert werden. Der Upload in einen App Store verkürzt das Vorgehen wesentlich.

- Vertriebskanal: Neue Software braucht vom Unternehmen nicht an alle Mitarbeiter publik gemacht und verteilt zu werden. Nach dem Upload einer App in den Enterprise App Store können alle Mitarbeiter diese App im Store sehen. Eine entsprechende Benachrichtigung über eine MDM-Lösung kann den Vorgang zudem beschleunigen.

- Feedback: Mitarbeiter haben genau wie in öffentlichen App Stores die Möglichkeit, die vom Unternehmen zur Verfügung gestellten Apps zu bewerten und Rezensionen abzugeben. Das Unternehmen kann dieses Feedback nutzen, um schnell auf die Wünsche der Mitarbeiter und Probleme mit den Apps zu reagieren.

- Lizenzen statt Produkte: Das Unternehmen kauft und verwaltet Lizenzen und keine Produkte mehr (CDs, DVDs, …).

- Inhaltskontrolle: Bei einem Enterprise App Store kann das Unternehmen über den Inhalt des Stores entscheiden. Es können unerwünschte Apps ausgeschlossen und neue Apps hinzugefügt werden.

Nachteile für Mitarbeiter:

- Plattformabhängigkeit: Viele App Stores sind abhängig von der darunterliegenden Plattform. So ist Google Play Store auch nur für Android-Geräte verfügbar und kann auch nur diese mit Apps versorgen. In dem Fall haben Mitarbeiter mit iOS-Geräten keinen Zugriff auf den Store.

- Versionszwang: Im App Store ist stets die neueste Version von Apps verfügbar. Wenn ein Mitarbeiter lieber mit einer älteren Version arbeiten möchte, so ist diese nach Erscheinen einer neueren Version nicht mehr aus dem App Store beziehbar.

- Inhaltsfilterung: Apps die vom Admin nicht in den App Store zugelassen werden, sind dort auch nicht verfügbar. Eine solche Not macht erfinderisch. Die Mitarbeiter könnten Apps, die im App Store nicht verfügbar sind, über Sideloading auf ihre Geräte laden. Der Admin sollte hierfür mit einer MDM-Lösung ausgestattet sein, die so etwas erkennt.

Nachteile für das Unternehmen:

- Inhaltskontrolle: Das Unternehmen ist verantwortlich für den Inhalt in einem App Store. Damit verbundene Entscheidungs-, Test- und Zulassungsprozesse benötigen ein entsprechendes Management.

- Abgaben an App Store: Sogar wenn man unternehmensintern kostenpflichtige Apps anbietet, ist man bei vielen App Store Lösungen zu einer Teilabgabe (ca. 30%) des dadurch entstehenden Umsatzes verpflichtet.

- Quellcodekontrolle durch Dritte: Wenn der App Store nicht vom Unternehmen selbst betrieben wird, sondern beispielsweise von Google, so wird der Quellcode beim Einstellen einer unternehmensinternen App, genau wie alle anderen eingestellten Apps, auf Malware und Viren überprüft. Hierzu wird u.a. der Quellcode der App eingesehen, was durchaus als sicherheitskritisch eingestuft werden muss.

- Nicht-Zulassung/Löschung von Apps: Wenn der App Store nicht vom Unternehmen selbst betrieben wird, so können Apps, ob unternehmensintern oder nicht, vom App Store Betreiber nicht in den App Store zugelassen oder sogar zu einem beliebigen Zeitpunkt aus dem Store gelöscht werden.

Es gibt also ohne Zweifel Gründe für Unternehmen, sich über einen eigenen App Store Gedanken zu machen. Diese Gründe kann man wie folgt zusammenfassen:

- Unternehmenseigene Apps: Wenn Apps, die für das Unternehmen entwickelt wurden, über einen öffentlichen App Store an alle Mitarbeiter vertrieben werden, so haben auch alle anderen App Store Besucher Zugriff auf diese Apps. In einem öffentlichen App Store können Apps nicht nur für bestimmte Benutzer zugänglich gemacht werden. Sie können dann höchstens auf einen bestimmten Gerätetyp (z.B. iPad) oder ein Land beschränkt werden.

- Sicherheit: Die Betreiber von App Stores überprüfen alle neuen Apps und alle Updates bis auf Quellcode-Ebene. Falls eine unternehmensinterne App nach dem Starten als erstes einen Authentifizierungsdialog anzeigt, bei dem sich nur berechtigte Mitarbeiter autorisieren können, so wird die App für keinen der großen App Stores zugelassen. Diese müssen jede App in ihrem vollen Funktionsumfang testen können. Sie raten daher in solchen Fällen einen Test-Account anzulegen mit bereinigten Daten und die Anmeldedaten für diesen Account bei dem Upload der App mitzuschicken. So kann der App Store-Betreiber die App trotz Authentifizierungsdialog vollständig testen. Dabei können jedoch auch die Authentisierungsmechanismen der unternehmenseigenen App, sowie ihre Funktionsweise und etwaige wiederverwendete Bibliotheken aus entsprechenden Desktop-Versionen von Dritten eingesehen werden. Ein uneingeschränkter Zugriff auf alle Apps eines öffentlichen App Stores trägt aufgrund der hohen Anzahl von Malware-Apps und Viren ebenfalls zu Sicherheitsbedenken bei.

- Gerätekontrolle: Während öffentliche App Stores höchstens die Einschränkung der App auf bestimmte Gerätetypen und Länder zulassen, bieten Enterprise App Stores auch die Möglichkeit Apps nur für bestimmte Geräte einer Abteilung (z.B. Controlling) zuzulassen. Zudem können sie im Zusammenspiel mit MDM und Mobile Application Management (MAM) die letzte aus dem App Store heruntergeladene Version einer App einsehen und durch entfernten Zugriff auf das Endgerät Anwendungen und Updates pushen und erzwingen.

- Policies: In einem unternehmenseigenen App Store kann man selbst Regeln definieren, welche Apps in den Store aufgenommen werden und welche nicht. Zudem kann man Patch- und Update-Regeln definieren. So könnten große Updates nur bei einem Zugriff von einem WLAN aus auf das Handy übertragen werden. Datenupdates mit sensiblen Daten könnten sogar nur auf das unternehmenseigene WLAN beschränkt werden. Sicherheitskritische Updates könnten unmittelbar über das mobile Netz übertragen werden.

- Rollouts & Updates: Während man bei einem offiziellen App Store auf die Kontrolle und Freigabe des App Store-Betreibers warten muss, können unternehmensinterne Apps im Enterprise App Store unmittelbar für alle Mitarbeiter bereitgestellt werden.

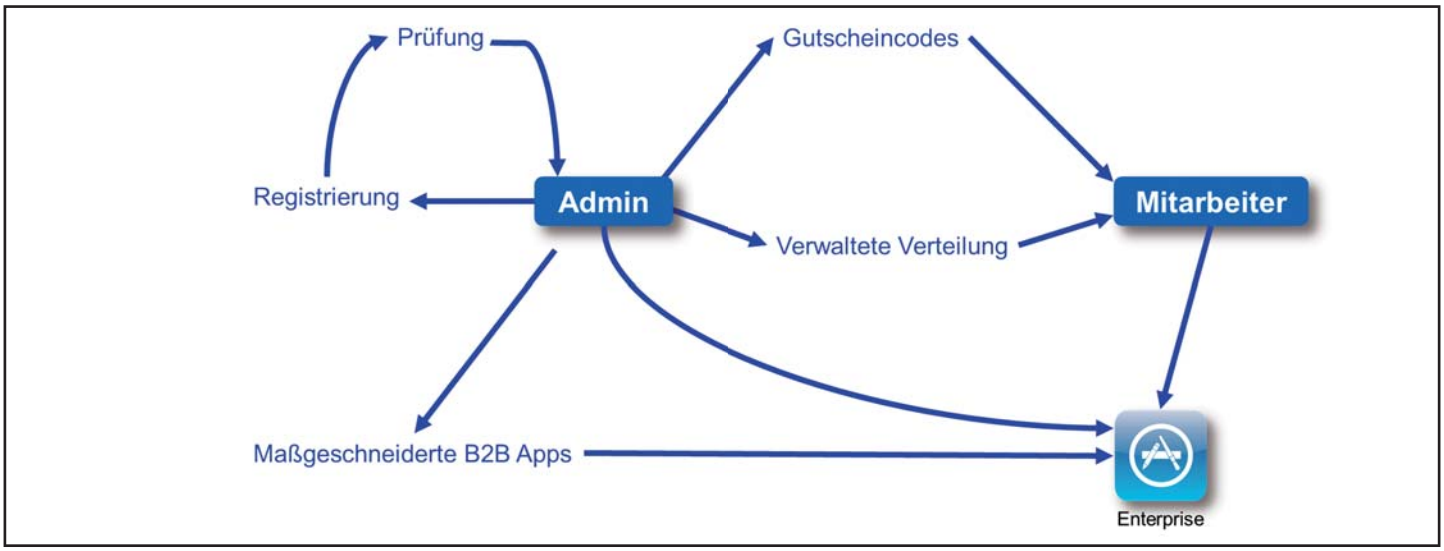


Abbildung 3: Apple Enterprise Volume Purchase Program

Apple Enterprise Volume Purchase Program

Ein Beispiel für eine weit verbreitete Möglichkeit Apps in Unternehmen zu kaufen und zu verteilen ist Apples Volume Purchase Program (VPP) für Unternehmen (siehe Abbildung 3). Damit dieses Programm dem Unternehmen zur Verfügung steht, muss der Admin zunächst das Unternehmen bei dem US-amerikanischen Unternehmensverzeichnis Dun&Bradstreet anmelden. Hierzu gehören eindeutige Informationen über das Unternehmen wie Anschrift, Kontaktinformationen sowie die Umsatzsteuer-ID, damit man in Europa umsatzsteuerfrei Apps kaufen kann. Anschließend erfolgt durch den Admin die Anmeldung des Unternehmens beim VPP Programm. Dabei gleicht Apple die Angaben mit Dun&Bradstreet ab, überprüft die Konformität auf steuerliche Richtlinien des jeweiligen Landes und sendet dem Admin nach erfolgreicher Prüfung eine AppleID zu, die dem Unternehmen zugeordnet ist. Dies ist insofern etwas Besonderes, da AppleIDs i.d.R. einer Person zugeordnet sind. Bei der Registrierung der unternehmenseigenen AppleID darf keine E-Mail Adresse verwendet werden, die bereits zur Registrierung einer anderen AppleID verwendet wurde. Nach erfolgreicher Registrierung kann der Admin beginnen, Apps für den Enterprise App Store zu kaufen. Dabei sucht er sich die App aus, bestimmt die Anzahl der Lizenzen und den Verteilungstyp. Als Zahlungsmethoden stehen in Deutschland Kreditkartenzahlung sowie ClickAndBuy zur Verfügung. Der Kauf wird anschließend via E-Mail bestätigt. Der Admin kann jederzeit den Einkaufsverlauf, Status der Einkaufslizenzen sowie der Transaktionen einsehen.

Es gibt zwei Möglichkeiten Apps aus dem VPP an Mitarbeiter zu verteilen. Eine Methode besteht aus dem Versenden von Gutscheincodes. Die Mitarbeiter müssen anschließend auf einer Webseite den Gutscheincode sowie ihre persönliche AppleID und ihr Kennwort angeben. Daraufhin wird die App für den Mitarbeiter freigeschaltet und er kann diese auf seinem Apple-Gerät installieren. Der Vorteil eines solchen Vorgehens ist, dass auch externe Mitarbeiter auf diesem Weg mit Apps versorgt werden können. Ein Nachteil dieser Variante ist die Tatsache, dass die App Lizenz so an die jeweilige AppleID des Mitarbeiters übertragen wird. Die vom Unternehmen gekaufte App ist anschließend vollständig im Besitz des Mitarbeiters. Wenn er das Unternehmen verlässt, so nimmt er die App und die Lizenz mit. Bei der zweiten Methode, unter Einbeziehung einer MDM-Lösung, ist dies nicht der Fall. Bei der sog. verwalteten Verteilung spielt ein MDM eine zentrale Rolle. Dieses MDM kann entweder das eines Drittanbieters sein oder der Apple Profile Manager. Über das MDM können sich Mitarbeiter mit ihrer persönlichen AppleID und ihrem Gerät anmelden. Dem Admin bleibt die persönliche AppleID der Mitarbeiter stets verborgen. Er kann jedoch die Geräte der Mitarbeiter einsehen. Die Lizenzen kann der Admin unmittelbar den Geräten der Mitarbeiter zuschreiben. Über die MDM-Lösung kann der Admin alle Mitarbeiter mit Push-Notifications über die für sie zur Verfügung stehende App benachrichtigen. Dabei bleibt die Lizenz allerdings Eigentum des Unternehmens. Wenn ein Mitarbeiter mit seinem Endgerät das Unternehmen verlässt, so kann die MDM Lösung entweder die App unmittelbar von dem Gerät des Mitarbeiters löschen oder die Lizenz entziehen. Wenn die Lizenz entzogen wird, so wird der Mitarbeiter darüber informiert und kann die App weitere 30 Tage nutzen. In dieser Zeit kann er selbst eine Lizenz der App erwerben und die App somit weiterhin privat nutzen. Erwirbt er in der Zeit keine eigene Lizenz, so wird die App von seinem Gerät automatisch nach 30 Tagen gelöscht. Der Admin kann die Lizenz unmittelbar nach dem Widerruf an einen anderen Mitarbeiter verteilen. Nach der Zuteilung der App kann der Mitarbeiter alle ihm verfügbaren Apps in dem Enterprise App Store einsehen.

Neben dem Kauf und der Bereitstellung bereits verfügbarer Apps des App Stores bietet das Enterprise VPP auch noch die Möglichkeit, maßgeschneiderte (unternehmensinterne) Apps im eigenen Enterprise Store anzubieten. Hierzu beauftragt der Admin eine Entwicklerfirma, die in Besitz einer Enterprise Entwicklerlizenz für 299$ ist. Nach der Entwicklung der unternehmenseigenen App kann der Admin diese bei der Entwicklerfirma kaufen und wie gewohnt zum Enterprise App Store hinzufügen. Die berechtigten Mitarbeiter finden diese App wie gewohnt zum Download im Enterprise App Store.

Google Play Private Channels

Google bietet mit den Google Play Private Channels eine andere Möglichkeit für Unternehmen ihre eigenen Anwendungen zu vertreiben (siehe Abbildung 4). Der Private Channel fügt der kategoriengeprägten Ansicht bei Googles App Store eine weitere Kategorie hinzu. Diese Kategorie ist beschriftet mit dem Unternehmensnamen wie er bei der Google Apps Domain angegeben wurde (siehe Abbildung 5). Google Play Private Channel wird in Zusammenhang mit den Google Apps Domains vertrieben. Dabei darf jedes Unternehmen genau einen Private Channel haben. Der Admin muss hierzu über die Google Apps

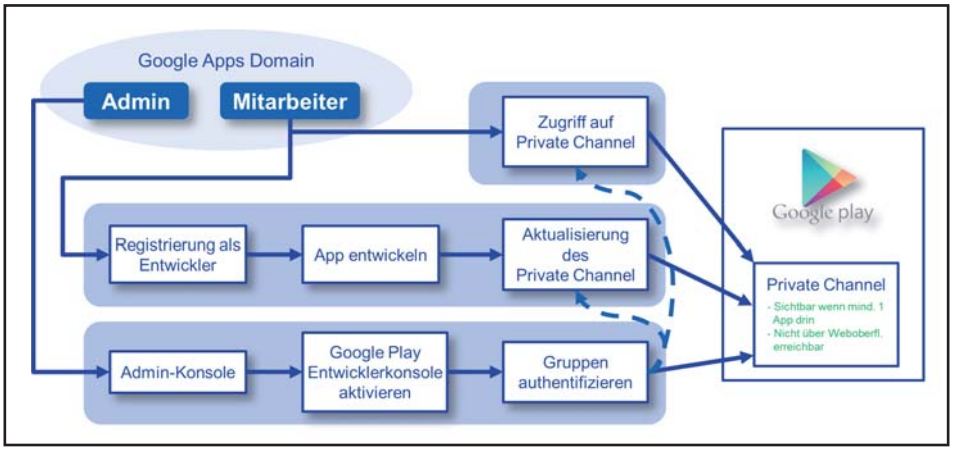


Abbildung 4: Google Play Private Channels

Domain Admin-Konsole die Google Play Entwicklerkonsole aktivieren. Anschließend kann er sowohl Entwickler dazu bemächtigen Apps in den Private Channel zu laden, als auch Mitarbeiter autorisieren bestimmte Apps herunterladen zu können.

Jeder Mitarbeiter, der in der gleichen Google Apps Domain registriert ist, kann sich als Entwickler für den Private Channel registrieren. Die Entwicklerlizenz für Googles Play Store kostet einmalig 25$. Nach der Entwicklung der App und Authentisierung durch den Admin kann der Entwickler Apps in den Private Channel stellen. Die Mitarbeiter können nach der Zuteilung durch den Admin Apps im Private Channel einsehen und auf ihren Geräten installieren. Allerdings können im Private Channel keine Apps angeboten werden, die auch im öffentlichen Store verfügbar sind. Wenn das Unternehmen seinen Mitarbeitern also auch Apps aus dem öffentlichen Store anbieten will, so muss der Zugriff auf den öffentlichen Store gewährt werden.

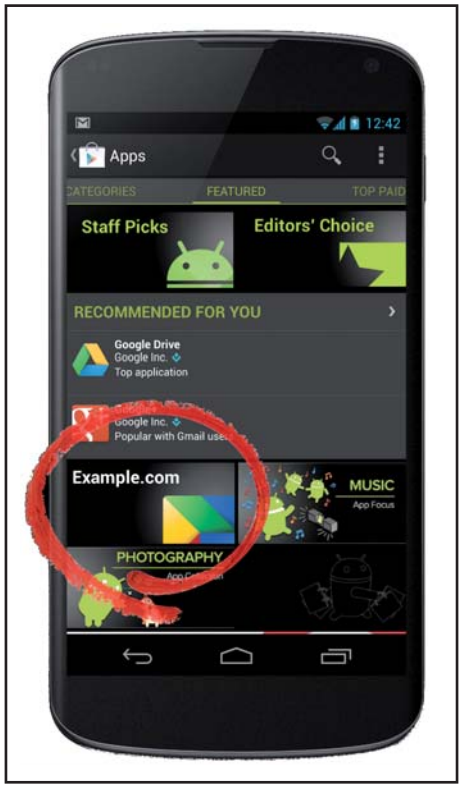


Abbildung 5: Beispiel eines Private Channels
Quelle: Google

Private Channel Hin oder Her

Ein Nachteil des Private Channels ist der Fokus auf das Android Betriebssystem. iOS Geräte können mit einer solchen Lösung nicht bedient werden. Ein weiterer Nachteil ergibt sich aus der Tatsache, dass Apps für den Private Channel auf die gleiche Art und Weise durchleuchtet werden wie Apps für den öffentlichen Store. Es kann dabei zudem geschehen, dass eine App für den Private Channel nicht zugelassen wird, da sie den Anforderungen von Google (z.B. in Bezug auf Design oder Sicherheit) nicht ausreichend nachkommt. Vorteile ergeben sich beispielsweise aus der in Google verankerten Nutzerauthentifizierung und der Mitnutzung des Google Play Abrechnungssystems. Man benötigt hierfür also kein eigenes Abrechnungssystem und ggf. auch keine separate Nutzerauthentifizierung innerhalb der Apps, da diese auch nur Nutzer installieren können, denen der Admin Zugriff auf die App gegeben hat. Über das im Google Play Store integrierte Bewertungssystem können die Mitarbeiter auch geschäftsinterne Apps auf die gewohnte Art und Weise bewerten und an zentraler Stelle Kritik äußern.

App Verteilung ohne App Store

Als alternative Verteilungsmöglichkeiten neben App Stores gibt es Jailbreaking und Sideloading. Beim Jailbreaking beschafft sich der Besitzer des Endgerätes Root-Rechte und kann dadurch anschließend beliebige Apps auf dem Gerät installieren und entfernen. Für das Sideloading sind keine Root-Rechte notwendig. Bei Android reicht dafür ein Häkchen unter den Einstellungen für „Installation von Apps von anderen Quellen als Play Store erlauben“. Beide Methoden haben sowohl Vor- als auch Nachteile. Zu den Vorteilen gehört die Möglichkeit beliebige Apps (veraltet, nicht in App Store aufgenommen, …) zu installieren. Man ist also nicht auf die Apps im App Store beschränkt. Zudem kann man die Apps sehr leicht verteilen. Hierzu muss man lediglich die Installationsdatei über E-Mail, ein Netzlaufwerk oder einen Web-Download den Mitarbeitern zukommen lassen. Updates müssen anschließend auf gleichem Wege installiert werden. Die alte Version einer App wird dann schlicht mit einer anderen überspielt. So können Mitarbeiter auch nachträglich wieder alte Versionen einspielen. Während der Upload und die Verfügbarkeit einer neuen App in einen Store Zeit benötigen, kann dies beim Sideloading unmittelbar geschehen. (siehe Abbildung 6)

Bei diesen Methoden herrschen aber auch nicht zu unterschätzende Risiken. Während alle Apps in öffentlichen Stores zumindest den Überprüfungen der jeweiligen Stores unterliegen, können Apps beim Sideloading ohne jegliche Kontrolle auf Schadsoftware installiert werden. Wenn eine App auf einem Gerät mit Jailbreak läuft, kann sich diese im Prinzip durch Root-Rechte beliebige Daten des Gerätes sichern und versenden. Die üblichen Kontrollmechanismen greifen dann nicht mehr zuverlässig. Durch die manuelle Verteilung der Apps und Updates und die daraus re-

Abbildung 6: Alternative App Verteilung ohne App Stores

sultierende mangelnde zentrale Kontrolle (wie z.B. bei einem App Store) und Monitoring der Versionen (App Store in Kombination mit MDM) kann es zu einem starken Wildwuchs unter den Softwareversionen auf den Mobilgeräten kommen. Versionen mit erheblichen Sicherheitslücken können ohne Updates unerkannt auf Geräten verbleiben und jederzeit sogar auf noch ältere Versionen umgestellt werden. Obwohl Sideloading zwar auf allen aktuellen Plattformen wie Android, iOS und Windows Phone möglich ist, kann man aus den genannten Gründen insbesondere im Unternehmensumfeld davon nur abraten.

Enterprise App Stores trotz Gerätevielfalt

Die Probleme bei den bisher vorgestellten Lösungen beginnen bei zwei unterschiedlichen Plattformen in einem Unternehmen. Dabei gibt es auch für diese Fälle bereits bewährte und bekannte Lösungen. Eine solche Lösung ist der Good Technology Enterprise App Store. Dieser App Store bietet Anwendungen für Android, iOS, Windows Phone und in HTML5. Er kann sowohl mit einem MDM als auch ohne betrieben werden. So können Apps genau wie bei Apples Enterprise VPP auch an externe Zulieferer verteilt werden. Es gibt hierfür eine Anbindung an Apples VPP. Man kann plattformübergreifend den App Store Login als Single Sign-on zur App-übergreifenden Autorisierung verwenden. Es besteht die Möglichkeit die Apps in dem Store zu branden, genau wie dem Store selbst mit dem eigenen Unternehmenslogo ein Branding zu setzen. Neben dem Vertrieb von Apps können auch Dokumente, Handbücher, Präsentationen, Bilder, Schulungsvideos etc. über den App Store vertrieben werden. Wie in den öffentlichen App Stores können Anwendungen von Mitarbeitern bewertet und kommentiert werden. Dabei können sowohl öffentlich verfügbare als auch eigene Apps angeboten werden. Über eine Active Directory Anbindung können Apps gezielt bestimmten Benutzergruppen zur Verfügung gestellt werden. Eine solche Lösung kann sowohl in einer private Cloud als auch on-premise gehostet werden.

Der Apperian Enterprise App Store bietet eine vergleichbare Lösung mit Fokus auf die Cloud an. Im Gegensatz zu der Good Technology Lösung liegen die Daten bei Apperian in der Cloud (nicht on-premise). Apperian bietet ebenfalls Single Sign-on an und vertreibt Android, iOS, Blackberry, HTML5 und hybride Apps. Hybride Apps bestehen aus einer HTML5 Anwendung in einer nativen Hülle, z.B. einer Browser-View mit HTML5 Content auf Android. Durch die native Hülle haben die Anwendungen Zugriff auf viele hardwarenahe Funktionen (z.B. GPS oder Hardwarebeschleunigung) und durch die HTML5-Basis ist der Funktionsteil der Anwendung sehr leicht (und häufig unmittelbar) auf andere Plattformen portierbar. Um nicht mehrere Codebasen entwickeln und pflegen zu müssen, geht der Trend bei der App-Entwicklung in Richtung Plattformunabhängigkeit und dabei ist HTML5 führend. Für ein Unternehmen, das eine dedizierte Anwendung für mehrere Plattformen entwickeln lassen möchte, weil manche Zielgeräte mit Android laufen und andere mit iOS, spart dieser Ansatz häufig Entwicklungszeit und -kosten. Neben Apps kann man über den Apperian Enterprise App Store auch Geräteprofile und E-Mail Konfigurationsprofile verteilen. Genau wie bei Good Technology kann man auch bei Apperian Update Notifications verschicken und den Store an ein Active Directory sowie an Apples VPP anbinden. Ein interessantes Feature ist Apperian App Remote Control. Mit diesem Feature können Anwendungen, welche über den App Store auf den Endgeräten installiert wurden, bei Problemen von Technikern des eigenen Unternehmens live eingesehen werden. Hierdurch können Admins beispielsweise Mitarbeitern, die Probleme mit ihren Endgeräten und Apps haben, helfen. Zudem arbeitet Apperian nach dem Freemium-Prinzip. Bei dem ApperianONE Programm haben Unternehmen die Möglichkeit, den App Store im vollen Funktionsumfang zu testen. Die Beschränkungen schreiben jedoch maximal eine einzige App im App Store sowie maximal 100.000 Downloads dieser App vor.

Flexible Kostenmodelle

Die Kosten für Enterprise App Stores teilen sich in monatliche sowie etwaige einmalige Posten auf. Die monatlichen Kosten bieten eine flexible Planung. Beispielsweise kostet die Nutzung von Google Play Private Channels 4€ pro Nutzer pro Monat oder alternativ 40€ pro Nutzer pro Jahr. Good Technology bietet den App Store für 5$ pro Nutzer pro Monat an. Weitere Anbieter bewegen sich im gleichen Preissegment. Die einmaligen Kosten entstehen zum Beispiel durch Publisher-Lizenzen. Diese werden benötigt, wenn man eigene Anwendungen in einen App Store laden oder entwickeln möchte. Solche Lizenzen kosten beispielsweise bei Google einmalig 25$ und bei Apple 299$ pro Jahr (iOS Developer Enterprise Program License).

Auswirkungen auf die Unternehmens-Infrastruktur

Viele der App Store Lösungen benötigen eine Anbindung an eine Public Cloud. Dies gilt insbesondere wenn der Enterprise App Store auch Zugriff auf Anwendungen aus einem öffentlichen App Store geben soll (z.B. Google Private Channel Lösung). Andere Vertriebsmöglichkeiten können unternehmensintern abgewickelt werden, wie beispielsweise Sideloading oder die Good Technology on-premise Lösung. Dabei fallen unterschiedliche Lasten auf die Infrastruktur an. App Stores werden auf Anwendungs-/Service-Ebene betrieben. Die Datenverbindung zu den Endgeräten erfolgt i.d.R. kabellos, entweder über WLAN oder über mobile Datenverbindungen. Da-

bei kann man je nach Lösung und MDM/MAM-Anbindung auch entscheiden, ob Updates

- aufgrund ihrer Größe ausschließlich über WLAN übertragen werden sollen, z.B. um das mobile Datenvolumen der Mitarbeiter nicht unnötig zu belasten,
- aufgrund sensibler Datenupdates ausschließlich im unternehmensinternen WLAN (oder über VPN) übertragen werden sollen oder
- aufgrund sicherheitskritischer Systemupdates unmittelbar über jede gerade verfügbare Verbindung vertrieben werden sollen.

Folgende Ereignisse können das mobile Datenvolumen oder das Unternehmensnetzwerk mehr oder weniger relevant belasten.

- Benachrichtigungen: Hierzu gehören Benachrichtigungen seitens des App Stores über verfügbare Updates, automatisch getätigte Updates und Änderungen an den Rechten von Apps. Diese Benachrichtigungen treten zwar häufig auf, aber das dadurch verursachte Datenvolumen ist sehr gering.
- Benutzeraktionen: Wie zum Beispiel sporadisches oder gezieltes Durchstöbern des App Stores nach neuen Apps. Solche Aktionen sind insbesondere in Bezug auf Enterprise App Stores selten, da sich dort im Gegensatz zu öffentlichen App Stores nicht so häufig etwas ändert. Das dadurch beanspruchte Datenvolumen ist ebenfalls gering.
- Installationen: Installationen beschränken sich auf die Kommissionierung neuer Endgeräte, Rollouts und das Neuaufsetzen von Geräten nach Abgängen von Mitarbeitern. Sie werden daher selten getätigt. Das Datenvolumen ist allerdings abhängig von der Größe der Apps. Wenn Apps bei der Installation ihren Datenbestand mitbringen, so wird hierfür ein entsprechendes Datenvolumen beansprucht.
- Systemupdates: Zu Systemupdates gehören Bugfixes, Feature- und Securityupdates. Die Häufigkeit solcher Updates hält sich in Grenzen. Das beanspruchte Datenvolumen pro Systemupdate kann höchstens so groß sein wie für die Installation der App.
- Datenupdates: Manche Apps laden ihre Daten zur Laufzeit nach. Diese benötigen eine ständige Verbindung zum Internet. Andere Apps bieten auch offline Funktionalität. Hierzu müssen die Daten offline verfügbar sein. Ein Beispiel aus dem Alltag sind Navigationssysteme, welche die Karten offline auf dem Gerät vorhalten. Diese ermöglichen zwar auch die Navigation ohne bestehende Internetverbindung, müssen jedoch hierzu regelmäßig Kartenupdates beziehen. Das Datenvolumen bei datenintensiven Apps, welche die Daten offline vorhalten, kann beliebig groß sein. Bei einer maximalen App-Datengröße bei Android von 4,05GB kann dabei einiges zusammenkommen. Je nach Größe und Wichtigkeit der Daten kann hier eine Beschränkung der Updates auf WLAN sinnvoll sein.

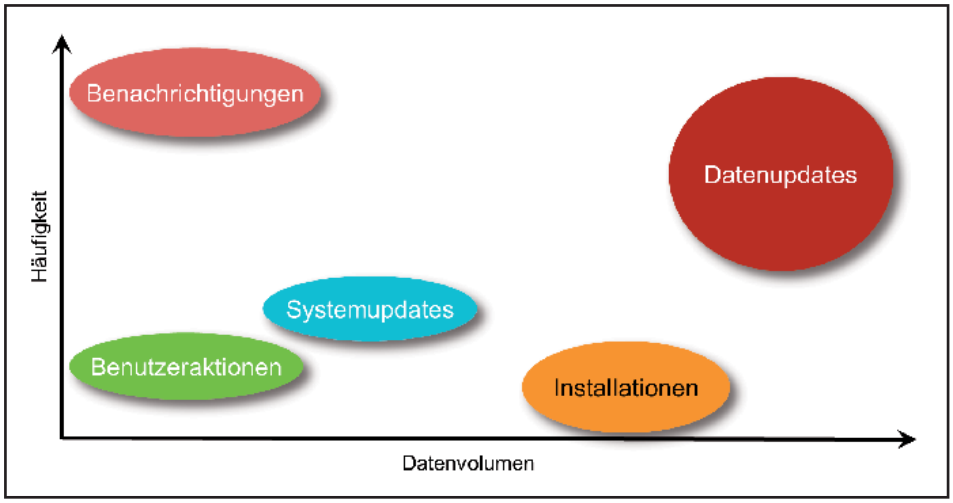


Abbildung 7: App Store Traffic

MAM vs. MDM

Gartner hat 2013 ein Wachstum von MAM zulasten von MDM vorhergesagt. Während MAM sich auf die Anwendungsebene beschränkt, haben MDM Lösungen weitreichendere Zugriffe auf Betriebssystemebene. So können MDM Lösungen i.d.R. nicht nur Anwendungen verwalten, sondern beispielsweise auch Passwortrichtlinien setzen, überprüfen und Betriebssystemupdates erzwingen.

App Stores spielen sowohl bei MAM als auch bei MDM eine Rolle. In Zusammenhang mit einer MDM Lösung sind diese jedoch wesentlich effizienter, insbesondere was Sicherheit angeht. Hierzu ein Beispiel: Angenommen ein Benutzer verwendet einen E-Mail Client aus einem Enterprise App Store. Mit diesem Client liest er E-Mails und speichert erhaltene pdf-Dokumente auf der SD-Karte um diese mit dem Endgerät lesen zu können. Wenn der Mitarbeiter das Mobiltelefon verliert, gibt es zwei unterschiedliche Möglichkeiten in Abhängigkeit von MAM oder MDM:

- **MAM:** Da der Mitarbeiter die E-Mail App aus dem Enterprise App Store bezogen hat, kann diese üblicherweise mit einer entsprechenden MAM-Lösung auch verwaltet werden. So kann der Admin die E-Mail App und den internen Speicher der App-Sandbox remote löschen. Er kann jedoch das pdf-Dokument, welches entweder auf der externen SD-Karte oder außerhalb der App-Sandbox auf dem internen Speicher abgelegt wurde, nicht löschen. Denn dieses Dokument ist nicht im Speicherbereich der App abgelegt. Somit ist der Inhalt des pdf-Dokumentes trotz MAM nicht vom Gerät löschbar.
- **MDM:** Unabhängig davon, ob der Mitarbeiter die App aus dem Enterprise App Store bezogen hat oder nicht, kann der Admin sowohl die App als auch den Inhalt des internen und externen Speichers remote löschen. Durch die tiefen Eingriffe einer MDM Lösung sind solche Eingriffe möglich.

Fazit

App Stores sind der Standard Vertriebsweg für mobile Anwendungen. Sie sind aus Sicherheits- und Zeitgründen dem Sideloading vorzuziehen. Die Verwendung von öffentlichen App Stores kann weitere Risiken mit sich bringen. Zum einen werden unternehmensinterne Anwendungen bei der Einstellung in den App Store vollständig durchleuchtet und zum anderen kann ein uneingeschränkter Zugriff auf alle Apps in einem öffentlichen App Store als Einfallstor für Schadsoftware dienen. Unternehmenseigene App Stores treten dieser Problematik entgegen und stellen in Kombination mit einer MDM-/MAM-Lösung ein umfassendes Konzept zur Verteilung und Management von Apps bereit.

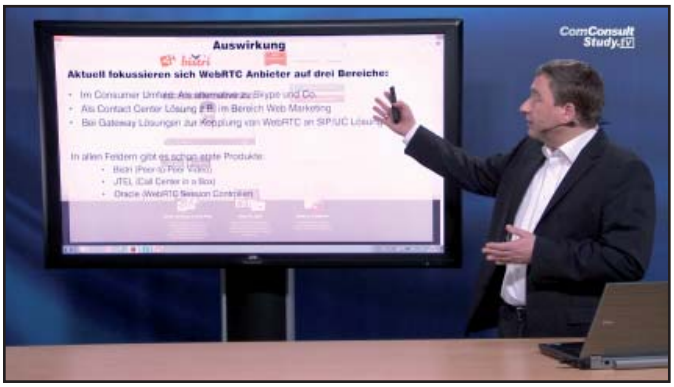
ComConsult-Study.tv

Mobile Devices Spezial im Mai bei ComConsult-Study.tv

Tablets, Smartphones, Phablets bieten Vor- aber auch Nachteile beim Einsatz im Unternehmen. In dieser Sammlung von Videos werden die Möglichkeiten der Geräte von ausgewiesenen Experten vorgestellt und bewertet. Ferner wird erläutert, wie App Stores Sinnvoll genutzt werden können und welche Alternativen es gibt. Abgerundet wird das Paket durch zwei Beiträge zu der aktuellen Entwicklung von WebRTC und den Chancen, die sich durch diese neue Technik eröffnen.

WebRTC: Funktionsweise, Standards und Codecs
Referent: **Markus Geller** Einzelpreis: 49,00 € netto
Zeit: 00:26:49 Im Abo: kostenlos

Der Markt der Videokonferenzlösungen wird durch die Entwicklung von WebRTC in eine neue Phase eintreten. Jetzt ist es zum ersten Mal möglich einen browserbasierten Client zu entwickeln, der auf allen nur denkbaren Endpunkten einsetzbar ist ohne Berücksichtigung der eingesetzten Betriebssysteme oder Laufzeitumgebungen. Dieser neue Ansatz wirft naturgemäß eine Reihe von Fragen auf.



WebRTC: die neue Art der Kommunikation
Referent: **Markus Geller** Einzelpreis: 49,00 € netto
Zeit: 00:21:22 Im Abo: kostenlos

Mit WebRTC etabliert sich ein neuer Standard für Sprach und Video Kommunikation auf Basis von Browser Technologien. So wie die SIP Signalisierung seit einigen Jahren den Markt der Enterprise TK-Systeme beherrscht, so zeichnet sich eine neue Art der Client Entwicklung mittels WebRTC ab.

Microsoft Surface Pro 2: besser als das iPad Air für Unternehmen?
Referent: **Dr. Jürgen Suppan** Einzelpreis: 59,00 € netto
Zeit: 00:52:12 Im Abo: kostenlos

Mit dem Surface Pro 2 bringt Microsoft nun zum ersten Mal ein Gerät, das hohe Erwartungen weckt. Ist hier zum ersten Mal eine Integration aus Tablet und Windows gelungen? Hat damit das iPad Air für Unternehmen an Bedeutung verloren?

Mobile Enterprise - Der Trend zu App Stores
Referent: **Dipl.-Inform. Dominik Franke**
Zeit: 00:43:00 Einzelpreis: 79,00 € netto
Im Abo: kostenlos

Mit mobilen Endgeräten ziehen auch App Stores in Unternehmen ein. App Stores können einerseits ein Einfallstor für ungewünschte und schädliche Software sein. Andererseits bieten sie aber viele Potentiale für die Verteilung und das Management von Apps auf Unternehmensgeräten.

Das Bundle bestehend aus den vier Videos für nur € 165,20*

*Dieses Angebot gilt nur im Mai 2014 .- Regulärer Preis € 236,-- netto

Weitere Details finden Sie auf unserer Homepage unter www.comconsult-study.tv

Standpunkt Sicherheit

Das Ende des Intranet

Der Standpunkt von Dr. Simon Hoff 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.

Getrieben durch die Anforderung, IT-Systeme und zugehörige Dienste und Anwendungen vom Server- bis zum Client-Bereich in „Sekundenschnelle“ zu provisionieren und dynamisch Ressourcen bereitzustellen, hat sich Cloud Computing in Verbindung mit Virtualisierungstechniken und Data Center Automation zu einem Standardelement der modernen IT entwickelt.

Dies wird nicht nur durch Konzepte wie den virtuellen Arbeitsplatz aus der Cloud deutlich. Smartphones und Tablets leben praktisch bauartbedingt von der Cloud. Apps verarbeiten und speichern ihre Daten in einer Cloud, Systemmanagement und Softwareverteilung (d.h. Mobile Device Management) erfolgen über eine Cloud. Diese Feststellung ist unabhängig von der Frage, ob es sich um eine Public Cloud, Private Cloud oder eine Hybrid Cloud handelt. Dort wo noch ein Fat Client benötigt wird, kommt dieser über eine Virtual Desktop Infrastructure (VDI) ebenfalls aus der Cloud.

Der Zugriff der Endgeräte auf Infrastruktur-Ressourcen erfolgt als Folge dabei verstärkt über das Internet und ein direkter lokaler Zugang wie für klassische PCs ist eigentlich nicht mehr erforderlich. Bei Smartphones und Tablets ist es sogar so, dass die Apps nicht mehr zwischen lokalem und remote Zugang unterscheiden (es sei denn, man zwingt die Systeme dazu).

Mit dieser Feststellung ergibt sich sofort die Möglichkeit (wenn nicht gar die Notwendigkeit) einer konsequenten Trennung von Clients und Servern, da Clients nur noch über Web-Applikationen oder Server-based Computing mit zentralen Ressourcen kommunizieren müssen. Hier kann die Kommunikation auf eine denkbar einfache Art und Weise entkoppelt über Firewalls und demilitarisierte Zonen (DMZs) erfolgen. Smartphones und Tablets würden beispielsweise für den WLAN-Zugriff im Intranet hierzu eine eigene Sicherheitszone erhalten, die nach angemessener Authentisierung den gewünschten Zugriff anbietet.

Damit wird deutlich, dass sich die Rolle des traditionellen Intranet als interner vertrauenswürdiger Netzbereich massiv geändert hat. Das Intranet zerfällt letztendlich in Sicherheitszonen unterschiedlicher Vertrauenswürdigkeit:

- Sicherheitszonen für eigene, vollständig kontrollierte Systeme
- Sicherheitszonen für Systeme, über die nur eine eingeschränkte Kontrolle besteht, wie z.B. Gebäudetechnik, sonstige Sondernetze, Netze für Systeme, die einem Outsourcing unterliegen (Printout Services, Unified Communications & Collaboration)
- Sicherheitszonen für Systeme, die vollständig außer der eigenen Kontrolle liegen

Unabhängig von der Einteilung in unterschiedliche Sicherheitszonen ist die Feststellung, dass sich Kommunikationsbeziehungen zwischen solchen Zonen oft nicht vermeiden lassen. Domänenkonzepte der Bauart Microsoft Windows / Active Directory passen hier nicht mehr und sind veraltet, da hier die Zugehörigkeit zu einer Domäne an die Zugehörigkeit zu einer gemeinsamen Sicherheitszone gebunden ist (und letztendlich eine vollständige Kontrolle der Systeme erforderlich ist). Andernfalls sind weitgehende Firewall-Freischaltungen nötig, die in modernen Rechenzentrums- und Campusnetzen immer weniger akzeptabel sind.

In der Extremform ist das Intranet von morgen also nichts anderes als ein „lokales Internet“, d.h. ein separates entkoppeltes Netz, dessen Zugangsmöglichkeiten zu den eigenen zentralen Ressourcen sich in nichts von einem Zugang über das Internet unterscheiden.

Interessanterweise ist diese Extremform aus dem Blickwinkel der Informationssicherheit ausgesprochen begrüßenswert. Wir können uns endlich auf den Schutz von Rechenzentrum und der dort verarbeiteten und gespeicherten Daten konzentrieren. Der flächendeckende Campus-Bereich kann mehr und mehr aus den Sicherheitsbetrachtungen ausgeklammert werden. Je weniger traditionelle Fat Clients dabei noch betrachtet werden müssen, desto leichter ist diese Trennung möglich.

Neues Seminar

Sonderveranstaltung: Internet of Things

23.06.14 in Köln

Die ComConsult Akademie veranstaltet am 23.06.2014 ihre "Sonderveranstaltung: Internet of Things" in Köln.

Wir stehen am Beginn einer der weitreichendsten Entwicklungen der IT. Es gibt bereits heute zahlreiche Lösungen und Produkte, welche IoT Szenarien in Unternehmen umsetzen und die Mehrwerte abschöpfen. Die Sonderveranstaltung gibt Einblicke in die Technologien hinter IoT, in verfügbare Produkte und existierende Lösungen. Auch die Tragweite der Gesamt-Entwicklung wird analysiert und ein Ausblick auf die Bedeutung dieser Technologie für die Zukunft der gesamten IT gegeben.

Während der chinesische Kalender das Jahr des Pferdes verkündet, läutet der IT-Kalender das Jahr des Internet of Things (IoT) ein. Wer die CeBIT oder die Embedded World besucht hat, wird es nicht abstreiten können. Ob die großen Global Player oder die Mittelständler mehr Trubel um das kommende Geschäft machen, ist schwer abzuschätzen. Aber die Anzahl bereits verfügbarer IoT Lösungen und Produkte ist beeindruckend und die strategische Ausrichtung der Unternehmen eindeutig.

Was genau ist an diesem Internet of Things so beeindruckend und wieso sehen alle hierin ein so großes Potential? Die Antworten auf diese Fragen sind ebenso zahlreich und unter-schiedlich wie die Versuche das Internet of Things zu definieren. Je nach Definition und Ein-satzbereich ist es entweder eine Art Schwarmintelligenz, bestehend aus einer losgelösten Wolke aus Sensoren und Aktuatoren, oder ein Haufen Cyber Physical Systems, welche Daten sammeln, aggregieren und mit Big Data-Ansätzen laufende Prozesse optimieren, oder aber ein Name für das Zeitalter, in dem es mehr Mikroprozessoren auf der Erde gibt als Menschen. Wie man es auch definiert, spätestens bei dem technischen und wirtschaftlichen Mehrwert sind sich alle einig. Der Preisverfall und die Miniaturisierung leistungsstarker Hardware, die Allgegenwärtigkeit des Internets, die flächendeckende Verfügbarkeit von Datennetzen (LTE, Wi-Fi, …) und der Einzug von IP in Industrie, Automatisierung und Kraftfahrzeuge eröffnet neue Einsatzszenarien und Geschäftsmodelle, welche die IT in den kommenden Jahren prägen werden.

Diese Sonderveranstaltung zu IoT beleuchtet grundlegende Technologien hinter IoT, informiert über laufende Initiativen und verfügbare Produkte von Herstellern und gibt einen Ausblick, wohin IoT die Industrie und Wirtschaft in Zukunft führen wird. Die Zuhörer bekommen bei der eintägigen Veranstaltung sowohl einen breiten Überblick über die gesamte IoT Landschaft, als auch ausgewählte tiefe technische Einblicke in essentielle IoT Grundlagen. Diese Veranstaltung beschränkt sich dabei nicht auf eine Branche, sondern bleibt insbesondere aufgrund der unterschiedlichen Qualifikationen der Vortragenden branchenübergreifend. Der Charakter der Veranstaltung fokussiert auf bereits verfügbare und eingesetzte Technologien im IoT-Umfeld, gibt jedoch auch visionäre Ausblicke, was uns noch alles erwartet.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Sonderveranstaltung: Internet of Things

Ich buche das Seminar

Sonderveranstaltung: Internet of Things

☐ am 23.06.14 in Köln
zum Preis € 990,-- netto

Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 14

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

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

Zweitthema

Vernetzte Hypervisor - Ein Einblick in virtuelle Switches im RZ-Umfeld

Fortsetzung von Seite 1

Dipl.-Inform. Sebastian Jansen hat Informatik mit dem Schwerpunkt „Verteilte Systeme“ an der RWTH Aachen studiert. Im Anschluss arbeitete er als wissenschaftlicher Mitarbeiter in Lehre und Forschung am „Lehrstuhl für Kommunikation und Verteilte Systeme“. Sein Forschungsschwerpunkt im „Ultra-Highspeed Information & Communication“ (UMIC) Exzellenz-Cluster lag dabei auf der Benutzerzentrierten Mobilität von Smartphone-Applikationen. Herr Jansen ist Berater bei der ComConsult Beratung und Planung GmbH in den Bereichen Data Center und User-centric Communications. Dort beschäftigt er sich im Projektgeschäft mit den Themen Server-, Client- und Netzwerk-Virtualisierung, Storage und Unified Communications.

Vor allem durch große Zahlen von VMs auf einzelnen Hosts wird diese Frage relevant, will (oder kann) man nicht jeder dieser VMs eine physikalische Anbindung an den entsprechenden, nächstgelegenen Switch zur Verfügung stellen.

Wir gehen in diesem Artikel der Frage nach, wie die aktuellen Antworten auf diese Frage aussehen, welche Vor- und Nachteile sie bieten und betrachten teilweise, wie sie bei den einzelnen Herstellern umgesetzt werden.

2. Switchvirtualisierung

In diesem Kapitel beschäftigen wir uns mit dem grundlegenden Konzept der virtualisierten Switches. Wir betrachten dabei die Unterschiede zwischen physikalischen und virtuellen Switches, Konzepte der Platzierung und Verteilung der virtuellen Switches (vSwitches), sowie die physikalische Netzanbindung und die verschiedenen Möglichkeiten des VLAN-Taggings in solchen virtualisierten Umgebungen.

2.1 Grundkonzept

In klassischen, d.h. nicht virtualisierten Umgebungen erfolgt der Anschluss eines Servers per Kupferkabel oder Lichtwellenleiter direkt an den jeweiligen Top-of-Rack- oder End-of-Row-Switch. Auf diese Weise erreicht man eine eindeutige Zuordnung eines Serverports zu einem entsprechenden Port auf Switchseite. Während beim gleichen Vorgehen bei einem Virtualisierungshost der Port auf Switchseite, nach wie vor, allein durch das Vorhandensein physikalischer Kabel und Stecker, eindeutig identifizierbar ist, verliert man eben jene Eindeutigkeit auf Seiten des Servers, da ein physikalischer Serverport nun zeitgleich mehreren virtuellen VMs-Ports zugeordnet ist, bzw. sein kann. Diese Zuordnung erfolgt, wie bei Virtualisierung üblich, über den jeweiligen Hypervisor des Hosts, der über seine Abstraktionsmechanismen die Netzwerkschnittstelle an die Clients weiterreicht. (siehe Abbildung 2.1)

Aktuelle Ansätze lösen dieses Problem durch das Zwischenschalten eines oder

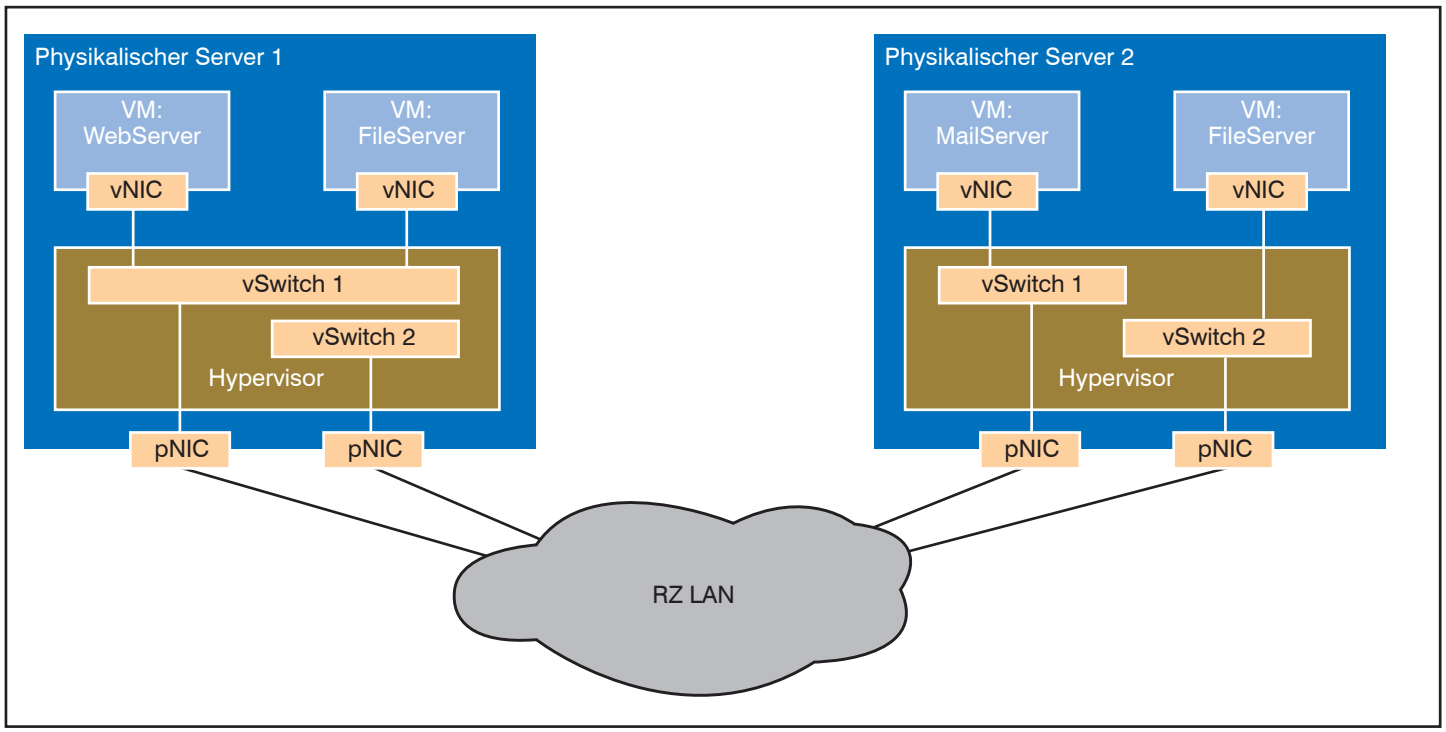


Abbildung 2.1: VMs sind mittels verschiedener vSwitches an das RZ LAN angeschlossen

mehrerer vSwitches auf Ebene des Hypervisors, denen die virtuellen Netzwerkschnittstellen (virtual network interface card – vNIC) der auf dem Host laufenden VMs zugeordnet werden. Auch eine Zuordnung verschiedener vNICs zu verschiedenen vSwitches ist so möglich, was es einerseits erlaubt VMs auf unterschiedliche Weise untereinander zu verbinden, bzw. sie andererseits in verschiedene Netze und Zonen im lokalen Netz zu integrieren. Eine rein Host-interne Vernetzung mehrerer VMs erlaubt beispielsweise den Aufbau von Testszenarien ohne Beeinflussung existierender Netze im RZ.

2.2 Unterschiede virtuelle / physikalische Switches

Aus der Sicht der Gastsysteme ändert sich oberhalb von Layer drei nichts im Vergleich zum Anschluss an einen physikalischen Switch, da der virtuelle Switch, wie bereits erwähnt, direkt im Hypervisor läuft und die Virtualisierung für den Gast damit weitestgehend transparent erfolgt. Auch nach außen, d.h. in das lokale RZ-Netz hinein, agiert der vSwitch wie ein herkömmlicher Switch.

Trotzdem gibt es einige Unterschiede in der Funktionsweise. So verwalten vSwitches beispielsweise keine dynamischen MAC-Tabellen. Da der „Anschluss“ der VMs an den vSwitch direkt mit der Konfiguration des Hypervisors erfolgt, handelt es sich hier um eine statische Zuordnung, was somit auch ARP-Requests überflüssig macht. Darüber hinaus erlaubt Paravirtualisierung der Gastsysteme (z.B. mit entsprechend installierten Erweiterungen und Tools) das Filtern von Broadcasts, sodass auf einer vNIC empfange Pakete nicht über andere vNICs weitergeleitet werden. Dieser Mechanismus verhindert das Kreisen von Paketen im (virtuellen) Netz, was gleichzeitig dazu führt, dass vSwitches sich nicht um Schleifenunterdrückungsprotokolle, wie z.B. SpanningTree, kümmern müssen.

2.3 Physikalische Anbindung & Lastverteilung

Eine weitere Herausforderung beim Anschluss mehrerer VMs an verhältnismäßig wenige physikalische NICs ergibt sich aus der Frage der Lastverteilung auf die einzelnen NICs durch den vSwitch. Bei nicht-virtualisierten Systemen stellt sich dieses Problem an dieser Stelle nicht, da ein Host entsprechend nur seine tatsächlichen Netzwerkadapter nutzen kann. Durch den Einsatz virtueller Switches besteht jedoch die Möglichkeit der Zuteilung mehrerer pNICs an VMs mit höherem Datenaufkommen.

Betrachtet man zuerst die Frage, welche NICs für eine Virtualisierungslösung relevant sind, fallen Schlagworte wie redundantes Management, Migration, Fehlertoleranz (*fault tolerance – FT*), Netzzugriff und ggf., falls nicht per *Host Bus Adapter (HBA)* realisiert, Speicherzugriff (ebenfalls redundant). Dabei sollten, neben dem Speicherzugriff, Migration und Fehlertoleranz, grundsätzlich getrennte Schnittstellen zur Verfügung stehen, da hier zeitweise besonders hohe Lasten zu erwarten sind. Bei einer physikalisch limitierten Zahl verfügbarer NICs kann das Maximum somit schnell erreicht werden. Durch geschicktes Kombinieren von aktiv/passiv-Rollen verschiedener Ports können hier jedoch Ports eingespart werden. So kann ein aktiver Management-Port gleichzeitig ein passiver Migrations-Port sein und umgekehrt. Im Regelbetrieb behindern die beiden Rollen sich damit nicht und erlauben die Verteilung auf nur zwei, anstelle von vier pNICs.

Nichtsdestotrotz ist die Zahl verfügbarer pNICs begrenzt und wenn man von Blade-Systemen mit maximal sechs pNICs ausginge, blieben, selbst ohne FT und bei Speicheranbindung mittels HBA, lediglich vier Ports für die reine Netzanbindung der VMs. Die Frage nach einer effizienten Verteilung der VMs auf diese pNICs bleibt also. Die Hersteller nutzen hier verschiedenste Ansätze um mit diesem Problem umzugehen.

2.3.1 VMware-Lastverteilung

VMware alleine bietet drei verschiedene Verfahren: *Originating Port ID, Source MAC Hash und IP Hash*.

Originating Port ID beschreibt eine gleichmäßige Verteilung der an einen vSwitch angeschlossenen vNICs. Die VMs werden dabei der Reihe nach an die pNICs angeschlossen. Erreicht man das Ende der pNIC-Liste, beginnt es nach einem Wrap-around wieder von vorne. Auf diese Weise erreicht man einerseits eine relativ einfache, konstante Verteilung, lässt aber andererseits auch die tatsächliche Last der einzelnen Maschine und Schnittstellen außen vor, sodass im ungünstigsten Fall mehrere VMs mit hoher Last über die gleiche pNIC nach außen geführt würden.

Bei ***Source MAC Hash*** werden Hashes auf Basis der MAC-Adressen der virtuellen Schnittstellen verwendet, um so eine möglichst gleichmäßige Verteilung der vNICs zu erreichen. Wie auch beim Originating Port Verfahren ergibt sich so eine konstante Zuordnung der Ports ohne Notwendigkeit der manuellen Konfiguration.

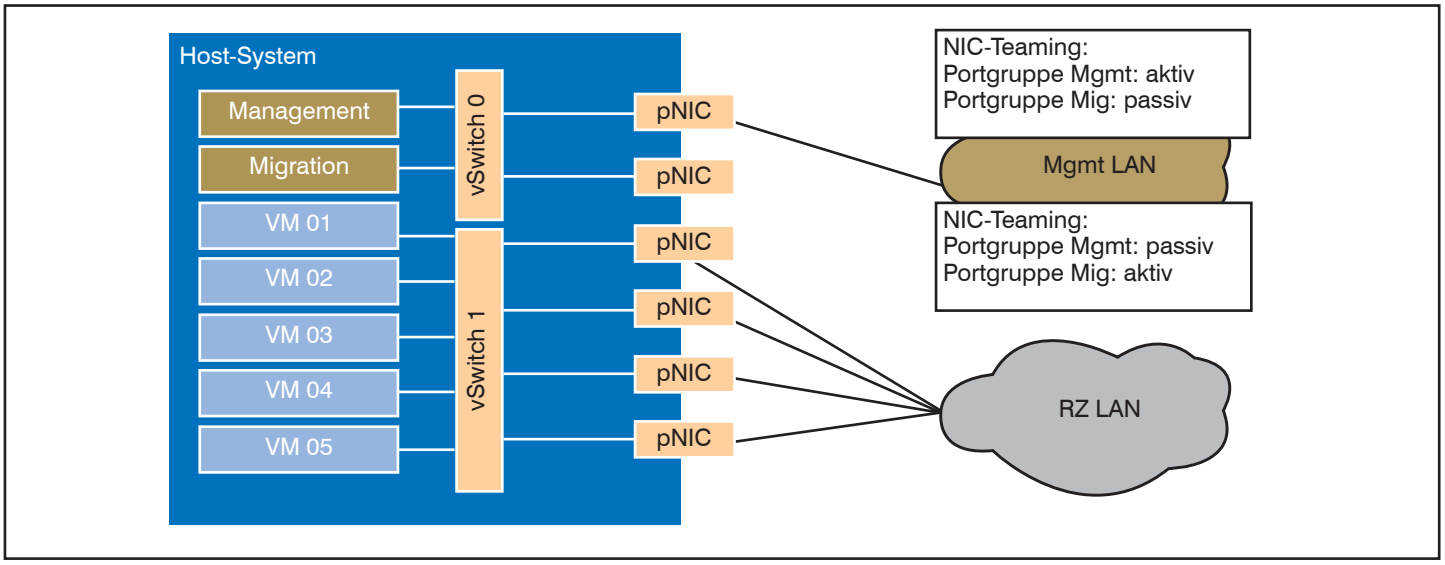


Abbildung 2.2: Eine mögliche Verteilung der vSwitches auf die physikalischen NICs des Hosts. Durch die Wahl der aktiv/passiv-Rollen ist es hier möglich zwei Ports doppelt zu belegen.

Allerdings lässt auch dieses Verfahren die tatsächliche Last der einzelnen Maschinen außer Acht. Zusätzlich kann es auch hier durch ungünstige Kollisionen zu einer Häufung von Maschinen auf einzelnen pNICs kommen.

IP Hash schließlich nutzt Hashes, die aus Quell- und Zieladresse der aktuellen Verbindung gebildet werden. Auf diese Weise ist die Zuordnung nur für die Dauer der aktuellen Verbindung konstant und wechselt mit hoher Wahrscheinlichkeit für die nächste Verbindung. Tatsächliche Lastbetrachtungen fallen damit auch hier aus. Sollten jedoch Maschinen hoher Last zufällig die gleiche pNIC nutzen, ist es wahrscheinlich, dass die Häufung bei der nächsten Verbindung nicht mehr auftritt.

2.3.2 Citrix-Lastverteilung

Citrix nutzt zur Lastverteilung das so genannte ***Source Level Balancing***. Dabei werden die VMs anhand ihrer MAC-Adressen auf die pNICs verteilt. Diese Verteilung wird dabei, auf Grundlage der aktuellen Lastsituation, in einem Round-Robin-Verfahren alle zehn Sekunden angepasst. Dementsprechend ändern sich hier auch regelmäßig die MAC-Adressen der vNICs, was das Verfahren durch ReverseARPs im Netz bekannt macht. Ggf. kann dieses Vorgehen jedoch zu Problemen führen.

2.3.3 Microsoft-Lastverteilung

Auch Microsoft verwendet mit dem ***Network Load Balancing*** ein Verfahren zur adaptiven Lastverteilung. Mittels NIC-Teaming werden dabei alle pNICs zusammengefasst und erhalten eine gemeinsame MAC-Adresse. Dies erfordert jedoch die Möglichkeit, MAC-Spoofing innerhalb der Gastsysteme zu aktivieren. Ein Nachteil dieses Systems ist, dass alle Pakete von außen immer an alle pNICs geflutet werden.

2.4 VLAN-Tagging bei virtualisierten Switches

Reden wir über vSwitches, so scheint der Weg zu VLANs nicht weit und auch wenn wir in diesem Artikel nicht primär über Zonenbildung oder Netzsegmentierung sprechen wollen, kommen wir an dieser Stelle nicht am Thema VLANs vorbei; konkreter: Am VLAN-Tagging. Da durch das Einführen von vSwitches in den Hypervisor das Thema VLANs und Mandantenfähigkeit hier auch schon eine Rolle spielt, muss auch der Aspekt der Bildung von VLANs in vSwitches berücksichtigt werden. Unabhängig von neueren Technologien wie *VMware NSX*, bei denen auf Basis der physikalischen Infrastruktur Overlaynetze zur Segmentierung genutzt werden, bietet das vSwitch-Umfeld drei Verfahren zur Bildung von VLANs.

2.4.1 Virtual Guest Tagging

Das ***Virtual Guest Tagging (VGT)*** verlagert das VLAN-Tagging vom Switch komplett in das Betriebssystem der virtuellen Maschine, d.h. beim Senden von Paketen muss der Gast die entsprechenden Tags setzen. Der Host wird damit automatisch von allen Tagging-Aufgaben befreit. Um Fehler zu vermeiden, muss hier sogar im Vorfeld das Tagging nach IEEE 802.1Q abgeschaltet und das Durchreichen des VLAN-Tags konfiguriert werden. Da die Konfiguration direkt auf dem Host passiert, gilt sie entsprechend für alle vSwitches auf dem so angepassten Host.

Im Gegenzug zur Entlastung des Hosts benötigt dieses Verfahren allerdings zusätzliche Kapazitäten und Prozessorleistung der jeweiligen Gastsysteme.

2.4.2 External Switch Tagging

Im Gegensatz zu VGT, wo eine Verlagerung nach innen erfolgt, verfolgt ***External Switch Tagging (EST)*** die entgegengesetzte Richtung mit einer Verlagerung nach außen. Hier übernimmt der Serverswitch, der an der physikalischen Schnittstelle angeschlossen ist, das Tagging auf Basis der Accessports. Voraussetzung dafür wiederum ist die Aufteilung aller vSwitches eines VLANs auf unterschiedliche pNICs des Hosts. Damit ist dieses Verfahren jedoch relativ unflexibel, sowohl in Bezug auf Lastverteilung als auch auf Erweiterbarkeit. (siehe Abbildung 2.3)

2.4.3 Virtual Switch Tagging

Während die beiden bisherigen Verfahren vor, bzw. hinter dem vSwitch ansetzen, arbeitet das **Virtual Switch Tagging (VST)** im vSwitch selber, was insofern sinnvoll erscheint, als dass hier für die

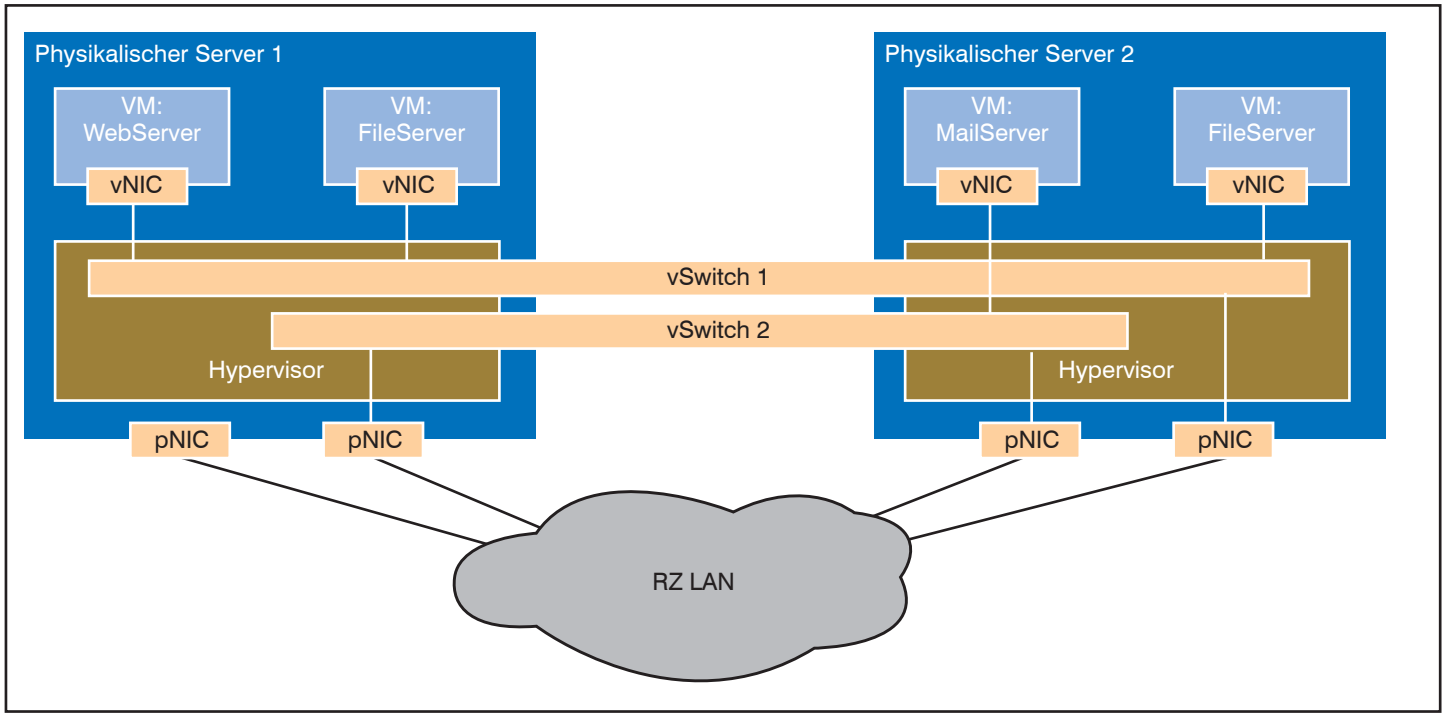


Abbildung 2.3: Ein verteilter, virtueller Switch überspannt über mehrere Hosts hinweg zwei Hypervisor und erlaubt so eine zentrale, konsistente Konfiguration selbst im Falle der Migration einer oder mehrerer VMs

VLANs der angeschlossenen VMs der erste Punkt ist, an dem mehrere Netze zusammenlaufen können.

Der jeweilige vSwitch wird dabei in verschiedene Portgruppen unterteilt, die dann den entsprechenden VLANs zugeordnet werden. Der vSwitch setzt dann bei den VMs ausgehenden Paketen die zugehörigen VLAN-Tags. Der Transport zum physikalischen Switch erfolgt über einen VLAN-Trunk. Auf diese Weise erreicht man die maximale Flexibilität, erhöht jedoch gleichzeitig die Komplexität der Virtualisierungsumgebung. Darüber hinaus beinhaltet dieser Ansatz das gleiche Problem, wie alle bisher vorgestellten vSwitch-Konzepte, nämlich die Tatsache, dass ein Teil der Netzwerk-Infrastruktur nicht durch die Netzwerker des Unternehmens administriert werden kann (siehe Kapitel 3 – Management).

2.5 Verteilung virtueller Switches

Bisher gingen wir davon aus, dass ein vSwitch sich genau innerhalb des Hypervisors eines Hosts befindet. Auf diese Weise kann jede beliebige VM dieses Hosts an diesen vSwitch angeschlossen werden. Bestimmte Szenarien, wie z.B. die Migration einer VM auf einen benachbarten Host im Cluster, können dieses Konzept allerdings an seine Grenzen bringen. Verändert die VM so ihren Standort, ist sie damit auch nicht mehr an ihren bisherigen vSwitch angeschlossen. Entsprechend müsste die VM auf dem Zielhost umkonfiguriert werden, damit sie dort an einem neuen vSwitch angebunden werden kann. Gleichzeitig muss der bisherige vSwitch erfahren, dass die VM nun nicht mehr an einem seiner virtuellen Ports zu erreichen ist.

Eine Möglichkeit diesen Problemen zu begegnen liegt darin, vSwitches Host-übergreifen zu konfigurieren. VMware bietet hier z.B. mit dem *vSphere Distributed Switch (vDS)* ein solches Konzept an; Citrix nutzt die *Open vSwitch* Technologie und Microsofts *Hyper-V Extensible Switch* unterstützt dieses Konzept ebenfalls. Durch eine Trennung von Data plane und Control plane (siehe auch Kapitel 3 – Management) erlaubt dieses System so eine über alle beteiligten Hosts verteilte, einheitliche Konfiguration, die auch mit entsprechenden Bewegungen zugehöriger VMs problemlos umgehen kann. Darüber hinaus reduziert die zentrale Konfiguration auch den Einrichtungs- und Wartungsaufwand, der bei vielen, einzelnen vSwitches vergleichsweise hoch wäre. Die so gewonnene Funktionalität und der Komfort kommen jedoch teilweise zu einem gewissen Preis, was z.B. im Falle von VMware eine höhere benötigte Lizenzstufe bedeuten würde.

3. Management

Wie man in Kapitel 2 sieht, existieren bereits einige Konzepte, die sich ausführlich mit den Themen und Problemen der Switch-Virtualisierung befasst und brauchbare Lösungen vorgestellt haben. Nichtsdestotrotz klang auch bereits mehrfach das Problem der Verwaltung und der Konfiguration an. Da die Virtualisierung klassischerweise in den Aufgabenbereich der Serververwaltung fällt, hat die Netzwerkadministration an dieser Stelle keinen Zugriff und Einfluss. Mit der Verwendung von vSwitches zur Anbindung der VMs an das restliche RZ-Netz kommt es damit zu einer Art Splittung des Netzwerks in zwei Teile. Der physikalische Netzwerkteil, der weiterhin durch die Netzwerker betreut wird und auf der anderen Seite die vSwitches, welche nun im Zuständigkeitsbereich der Server-Administratoren liegen.

Alternativ bietet sich die Möglichkeit, den Netzwerk-Administratoren Zugriff auf die Virtualisierungsinfrastruktur und das VM-Management zu ermöglichen, aber dieser Ansatz erfordert zusätzlichen Einarbeitungsaufwand durch die Netzwerker in die VM-Verwaltungswerkzeuge. Darüber hinaus ist diese Art der Einmischung in die Domäne des jeweils anderen auch selten gerne gesehen.

Zusätzlich stellt sich hier die wichtige Frage nach den konkreten Verantwortlichkeiten:

- Wer ist verantwortlich für den Netzzugang der VMs?
- Wer ist verantwortlich für das Management und die Wartung der virtuellen Switche?
- Wer ist verantwortlich für die korrekte Zuweisung der VMs zu ihren VLANs?
- Wie kann die Durchsetzung von Sicherheitsrichtlinien kontrolliert werden?

Die o.g. Punkte machen den Betrieb herkömmlicher vSwitches schwierig und führen zu Kompetenzgerangel und Schuldzuweisung zwischen den RZ-Teams im Fehlerfall. Hier bedarf es einer Lösung, die einen reibungslosen Betrieb und eine saubere Trennung der Zuständigkeiten zulässt.

3.1 Enterasys Network Access Control

Ein Ansatz zur Verwaltung der virtuellen Netzwerkinfrastruktur durch die Netzwerkabteilung bietet Enterasys (jetzt Extreme) mit ihrer Network Access Control (NAC). Das System, welches i.d.R. genutzt wird um Netzzugangskontrolle in Standardnetzen zu realisieren, wird hier eingesetzt, um die VMs der verschiedenen Hosts, beispielsweise mittels Authentisierung an

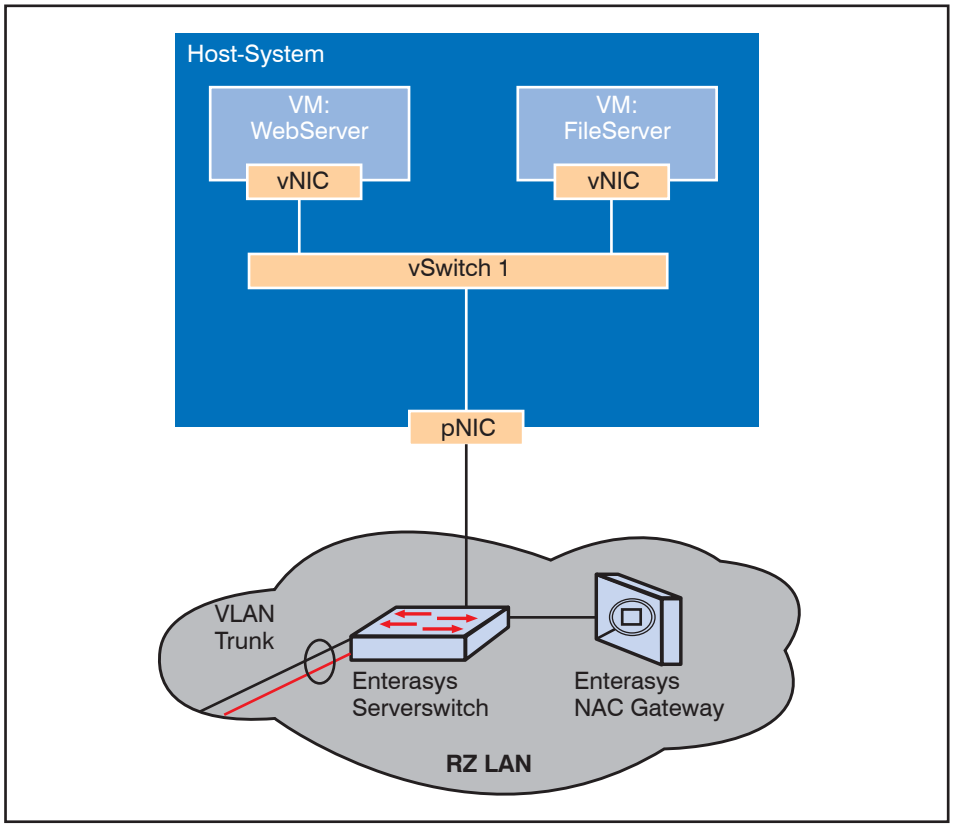


Abbildung 3.1: Der Verkehr der VMs wird über einen gemeinsamen vSwitch nach außen geleitet. Dort sorgt die Enterasys NAC für die Zuteilung der Pakete zu den entsprechenden Netzen.

RADIUS-Servern, o.ä. Mechanismen, zu den jeweiligen Servernetzen zuzuordnen.

Dieser Ansatz bietet zwar den Vorteil, dass keinerlei Eingriff in die Virtualisierungsumgebung von Nöten ist, greift allerdings auch erst in der physikalischen Infrastruktur. Im Vorfeld befinden sich daher alle Maschinen an einem vSwitch und damit innerhalb einer Broadcast-Domäne und es kann kein Eingriff bzw. keine Kontrolle erfolgen, was die Mandantenfähigkeit und Sicherheit innerhalb der Virtualisierungsumgebung zumindest fragwürdig erscheinen lässt. Es wird hier aber daran gearbeitet, die Lösung in die Netzwerk-APIs der VM-Anbieter zu integrieren. (siehe Abbildung 3.1)

3.2 Cisco Nexus 1000v

Eine andere mögliche Lösung basiert auf dem Konzept der verteilten vSwitches (siehe Kapitel 2.5). Durch die Trennung von Dataplane und Control plane wurde es ermöglicht, einen vSwitch über mehrere Hypervisor hinweg zu verteilen und gleichzeitig zentral zu konfigurieren. Nach wie vor liegt dabei die Kontrolle über diesen verteilten Switch aber in der Hand der Server-Administration.

3.2.1 Funktionsweise

Cisco hat sich dieses Problems angenommen und bietet mit dem Nexus1000v eine Lösung für dieses Dilemma. Der Nexus 1000v ist eine Weiterentwicklung der verteilten Switches und besteht im Wesentlichen aus zwei Teilen. Den *Virtual Ethernet Modules*, die in jedem zugehörigen Hypervisor installiert werden müssen und die Data plane bilden, auf der einen Seite und dem Virtual Supervisor Module (aus Redundanzgründen in doppelter Ausführung), einer virtuellen Switch-Appliance, die als Control plane zur Steuerung der VEMs dient, auf der anderen Seite. Alternativ zum Betrieb der VSMs als VMs auf einem Virtualisierungshosts bietet Cisco auch die Installation auf einer speziellen Appliance, der Nexus 1110er Serie an.

Der Cisco Nexus 1000v ersetzt dabei die standardmäßig vorhandenen Distributed Switches (z.B. vDS bei VMware). Normale, nicht-verteilte vSwitches, können aber weiterhin parallel dazu betrieben werden.

3.2.2 Integration

Der Vorteil des Nexus 1000v liegt dabei darin begründet, dass er sich wie ein herkömmlicher verteilter vSwitch in die Virtualisierungsumgebung integriert und somit auch die o.g. Aufgaben wie VLAN-Tagging etc. übernehmen kann, während er gleichzeitig als vollwertiger RZ-Switch der Nexus-Serie auftritt und per Nexus-OS vom Netzwerker konfiguriert und betrieben werden kann. Dies erlaubt dem Netzwerkteam vollständige Kontrolle über den

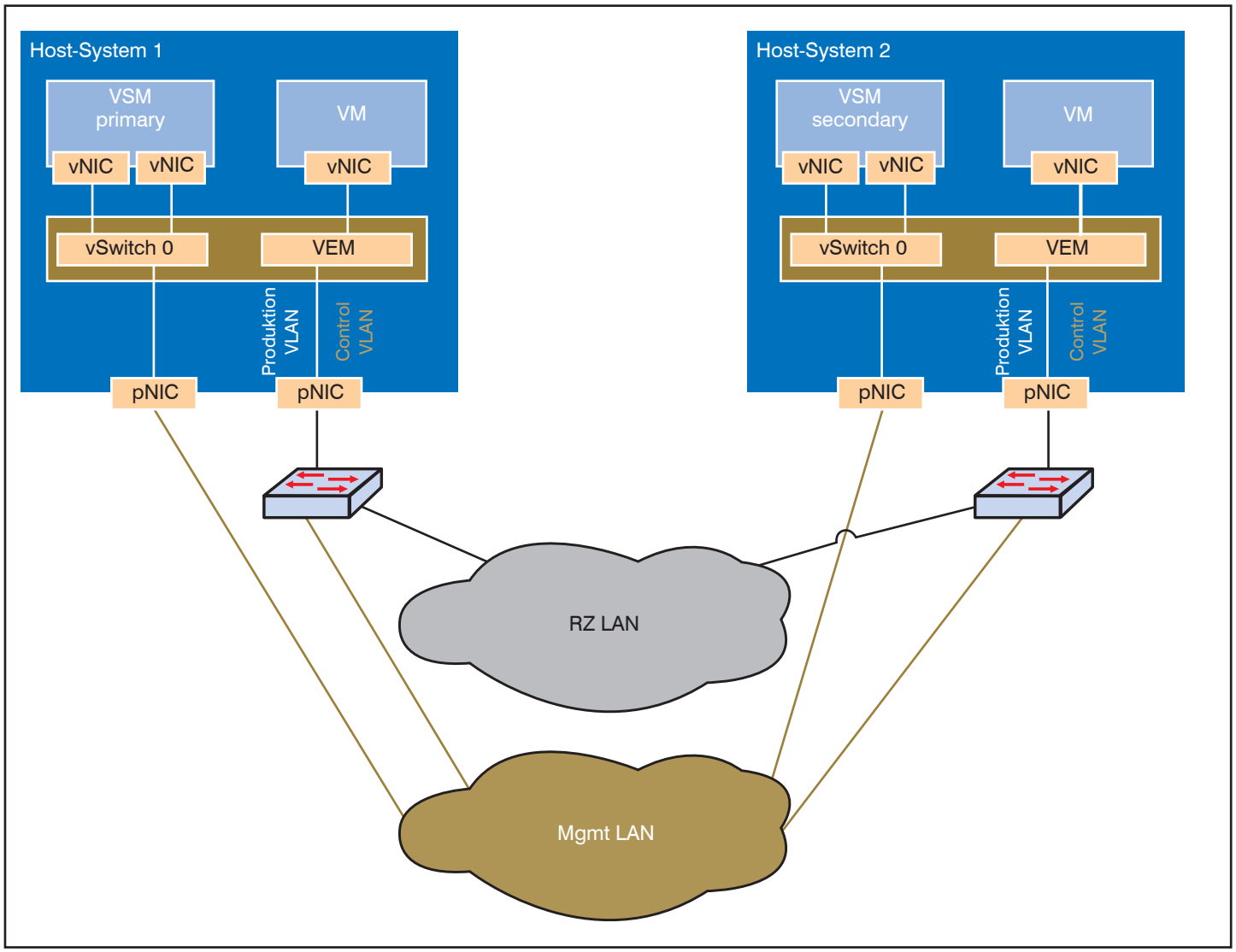


Abbildung 3.2: Der Cisco Nexus 1000v besteht aus der redundanten Control plane (VSM) und der über alle Hypervisor verteilten Data plane in From von VEM, die durch die VSM gesteuert werden.

Switch und die Ende-zu-Ende-Verbindungen zwischen VMs und anderen Maschinen des Netzwerks.

Der Nexus 1000v ist derzeit für VMware vSphere 5.x und Microsoft Hyper-V erhältlich. Eine Redhat KVM kompatible Version wurde jüngst angekündigt. (siehe Abbildung 3.2)

Zusätzlich ist zu beachten, dass für die Nutzung des Nexus 1000v unter VMware die höchste Lizenzstufe *Enterprise Plus* notwendig wird.

3.2.3 Lizensierung

Cisco bietet den NX1000v in zwei Lizenzstufen an, wobei in der Essential Edition bereits ein Großteil der Features kostenlos verfügbar ist. Lediglich für Sicherheitsfeatures wie *Cisco TrustSec* oder *IP Source Guard* wird die *Advanced Edition* notwendig, die mit derzeit 695$ pro CPU zu Buche schlägt.

3.2.4 Anmerkung

Mit dem *IBM System Networking Distributed Virtual Switch 5000v* schickte IBM 2012 einen Konkurrenten zum Nexus 1000v ins Rennen; dieser wurde jedoch zum 30. September 2013 vom Markt genommen und durch eine Overlay-Lösung, die *IBM System Networking Software Defined Network for Virtual Environments*, ersetzt.

3.3 Ausblick: Software-Defined Networking

Neben den beiden vorgestellten Ansätzen verschiebt sich die Entwicklung in diesem Bereich derzeit immer mehr in Richtung *Software-Defined Networks (SDN)* und alternativer Konzepte, z.B. durch Einsatz von Overlay-Netzwerken. Verstärkt wurde dieser Trend sicher durch die Akquise von Nicira durch VMware im Juli 2012 und die darauf folgende Entwicklung von *NSX* und *VXLAN*. Aber auch andere Projekte wie das *OpenFlow*-basierte *OpenDayLight*-Projekt forcieren ganz klar die Weiterentwicklung von SDN.

Das Konzept sieht dabei vor, auf die unterliegende, physikalische Netzwerkschicht ein virtuelles und unabhängiges Netzwerk zu legen. Dabei ist dieses so genannte Overlay-Netzwerk weitestgehend unabhängig von der unterliegenden Infrastruktur und kann somit rein in Software geplant und provisioniert werden, ohne dass Änderungen am physikalischen Netzwerk vorgenommen werden müssen. Auf diese Weise können innerhalb von kürzester Zeit neue Routen und Netze angelegt und bereitgestellt werden. Auch der Nutzen virtueller Switches würde damit verlorengehen, da eine einfache Verbindung der VM-Hosts zum physikalischen Netz genügen würde und der Rest wiederum im Overlay geschehen könnte.

Der Trend und die Entwicklungen in diesem Bereich stecken zwar derzeit noch in den Kinderschuhen, werden aber mit Sicherheit in naher Zukunft an Bedeutung gewinnen.

4. Fazit

Wie man sieht, ist die Virtualisierung längst kein reines Thema der Serverseite mehr. Durch die gewachsenen Anforderungen der Netzanbindung vieler virtueller Maschinen tritt das Feld virtueller Switches deutlich in den Fokus.

Das Mittel der Wahl hängt dabei ganz entscheidend vom jeweiligen Einsatzszenario ab. Für kleine Virtualisierungsumgebungen sind nicht-verteilte virtuelle Switches möglicherweise ausreichend und helfen dabei die Komplexität im überschaubaren Rahmen zu halten. Außerdem bietet der Einsatz dieser vSwitches häufig einen klaren Kostenvorteil, was die Lizensierung angeht.

Wird die Virtualisierungsumgebung größer und wächst die Zahl möglicher Migrationsziele einer VM im Cluster ebenfalls deutlich, führen nicht-verteilte Switches schnell zu sich wiederholenden Konfigurationen. Selbst kleine Änderungen an den jeweiligen Switches oder VMs können dann schnell großen Aufwand verursachen, wenn sie in jedem vSwitch nachvollzogen werden müssen. Hier sind verteilte virtuelle Switches ganz klar zu präferieren. Mit ihrer zentralen Konfiguration als Abstraktion der Control plane helfen sie dabei, ganze Cluster virtueller Maschinen von einer Stelle aus zu administrieren.

In den Fragen der Verwaltung und Administration solcher verteilter Switches weist der Cisco Nexus 1000v derzeit Alleinstellungsmerkmale auf. Als verteilter Switch in die jeweiligen Hypervisor integriert und mittels Nexus-OS basierter Control plane sorgt er für eine Netzwerk-basierte Kontrolle und Konfiguration des virtuellen Switches und erlaubt so gleichzeitig eine klare Abgrenzung der Zuständigkeiten und Verantwortlichkeiten von Netz- und Serveradministration.

Schließlich bleibt abzuwarten, wie sich der Bereich des Software-Defined Networking weiterentwickeln wird. Auch wenn die ersten Ansätze und Konzepte, die derzeit auf den Markt drängen, vielversprechend erscheinen, bleibt die Frage nach der Praktikabilität und Kosteneffizienz sowohl für KMU als auch für Enterprise vorerst offen. Aber wir sind uns sicher, dass das bei der derzeit stattfindenden, rasanten Entwicklung nicht lange so bleiben wird und viele Fragen in diesem Bereich bald beantwortet werden können.

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Ausschreibungen im Informations- und Kommunikationsbereich, 12.05.14 in Bonn

Dieses 1-tägige Seminar bietet einen praxisnahen Leitfaden für öffentliche Auftraggeber, die in ihren ITK-Vergabeverfahren unter Einhaltung aller gesetzlichen Auflagen das optimale Ausschreibungsergebnis erreichen wollen. Auch die Vertreter von Unternehmen lernen hier für ihre Ausschreibeungen die Rechts- und Investitionssicherheit zu verbessern und ein optimales Angebotsverhalten zu erreichen.

Preis: € 990,-- netto

Wireless LAN professionell, 12.05. - 14.05.14 in Bonn

Lernen Sie in diesem Seminar wie Sie eine WLAN-Lösung zukunftsorientiert und investitionssicher für die verschiedensten Endgerätetypen und Dichten aufbauen. Lernen Sie wie sie Verfügbarkeit und Bandbreite optimieren. Verbessern Sie Ihr WLAN mit den verschiedensten Struktur-Elementen vom Access-Point bis zum WLAN-Controller. Erfahren Sie worin sich Produkte und Technologien führender Anbieter unterscheiden. Berücksichtigen Sie die neusten Entwicklungen zur Gestaltung einer WLAN-Lösung, die langfristig tragfähig und wirtschaftlich ist. Lernen Sie Vor- und Nachteile aller aktuellen Technologien kennen und vermeiden Sie Planungs-Fehler.

Preis: € 1.890,-- netto

WAN: Konzept, Planung und Ausschreibung, 19.05. - 20.05.14 in Bonn

Seminar über die erfolgreiche Konzeption, Planung und Betrieb von WAN-Netzwerken. Lernen Sie wie Sie mit modernsten Technologien und erprobten Architekturen wirtschaftliche, verfügbare und leistungsfähige WAN-Lösungen aufbauen können. Erfahren Sie wie Sie sinnvoll SLAs für die Praxis aufsetzen können, die auch im Tagesbetrieb standhalten. Mit vielen Tipps und Tricks aus der Praxis.

Preis: € 1.590,-- netto

Trouble Shooting in vernetzten Infrastrukturen, 20.05. - 23.05.14 in Aachen

Dieses Seminar vermittelt, welche Methoden und Werkzeuge die Basis für eine erfolgreiche Fehlersuche sind. Es zeigt typische Fehler, erklärt deren Erscheinungsformen im laufenden Betrieb und trainiert ihre systematische Diagnose und die zielgerichtete Beseitigung. Dabei wird das für eine erfolgreiche Analyse erforderliche Hintergrundwissen vermittelt und mit praktischen Übungen und 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-Software kommt Wireshark zum Einsatz. Einer Verwendung selbst mitgebrachter Analyse-Software, mit deren Bedienung der Teilnehmer vertraut ist, steht nichts im Wege.

Preis: € 2.290,-- netto

Recht und Datenschutz bei Einführung von Voice over IP, 26.05. - 27.05.14 in Bonn

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 eine Überblick über den rechtlichen Rahmen zu geben beschäftigt sich dieses Seminar u.a. mit Fragen zur Abhörsicherheit, Vorratsdatenspeicherung, Datenverlust und den dazugehörigen Aspekten. Weitere Schwerpunkte bilden die etwaigen Vorgaben seitens der Bundesnetzagentur oder auch von Betriebsvereinbarungen, die es zu beachten gilt.

Preis: € 1.590,-- netto

Interne Absicherung der IT-Infrastruktur, 26.05. - 27.05.14 in Bonn

In diesem Seminar lernen Sie wie man die Sicherheit von LAN, WAN, Endgeräten, RZ-Bereichen, Servern und SAN erreicht. Konkrete Beispiele aus der Praxis zeigen den Weg zu einer erfolgreichen IT-Sicherheits-Lösung.

Preis: € 1.590,-- netto

Intensivtag: Tod des Tischtelefons und danach Cloud-Lösungen?, 27.05.14 in Bonn

Die Technologie für TK- und UC-Lösungen ist weiterhin in einem sehr schnellen Wandel begriffen. Gerade die zukünftige Rolle des Telefons und seine Umsetzung wird dabei von neuen Technologien immer mehr in Frage gestellt. Der Intensivtag widmet sich den Fragen nach der Zukunft des Telefons und der Endgeräte, dem Einfluss von WebRCT & Co, den Vor- und Nachteilen von Cloud-Lösungen und vergleicht TK und UC in ihrer Bedeutung für die Praxis. Es ist an der Zeit, Telefonie und UC-Lösungen neu zu positionieren und ein Maximum aus den neuen Möglichkeiten herauszuholen.

Preis: € 990,-- netto

RZ-RZ-Kopplung - alles nur eine Frage der Bandbreite?, 02.06.14 in Düsseldorf

Rechenzentren in entfernten Standorte zu betreiben erfordert sich mit IT-Sicherheit, Desaster Recovery, Service Level Agreements und Hochverfügbarkeit auseinander zu setzen. Dabei sind zum Teil Vorgaben bspw. vom BSI zu beachten. In dieser Schulung werden die aktuellen Techniken erläutert und für die richtige strategische Entscheidung zu einem Gesamtkonzept zusammengeführt.

Preis: € 990,-- netto

SIP (Session Initiation Protocol) - Basis-Technologie der IP-Telefonie, 02.06. - 04.06.14 in Düsseldorf

Ziel der Schulung ist die Erläuterung von SIP als den Schlüssel für eine offene, leistungsfähige und Kosten-optimale Kommunikations-Lösung. Es umfasst nahezu alle Dienste, die wir heute für UC benötigen: Sprache, Video, Daten und Präsenz. Lernen Sie was SIP leistet, worin sich wesentliche Hersteller-Lösungen unterscheiden und wie sie das Beste aus beiden Welten zukunftsorientiert nach ihrem Bedarf optimieren.

Preis: € 1.890,-- netto

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze
08.09. - 12.09.14 in Aachen
17.11. - 21.11.14 in Aachen

TCP/IP-Netze erfolgreich betreiben
02.06. - 04.06.14 in Aachen
20.10. - 22.10.14 in Aachen

Internetworking
23.06. - 27.06.14 in Aachen
03.11. - 07.11.14 in Aachen

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
20.05. - 23.05.14 in Aachen
28.10. - 31.10.14 in Aachen

Trouble Shooting für Netzwerk-Anwendungen
24.06. - 27.06.14 in Aachen
18.11. - 21.11.14 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
29.09. - 01.10.14 in Stuttgart
17.11. - 19.11.14 in Bonn

Session Initiation Protocol Basis-Technologie der IP-Telefonie
02.06. - 04.06.14 in Düsseldorf
20.10. - 22.10.14 in Berlin

Umfassende Absicherung von Voice over IP und Unified Communications
30.06. - 01.07.14 in Bonn
03.11. - 04.11.14 in Bonn

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
15.09. - 16.09.14 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: € 4.840,-- netto statt € 5.370,-- 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: insider@comconsult-akademie.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