ComConsult Research

Der Netzwerk Insider

April 2012

Systematische Weiterbildung für Netzwerk- und IT-Professionals

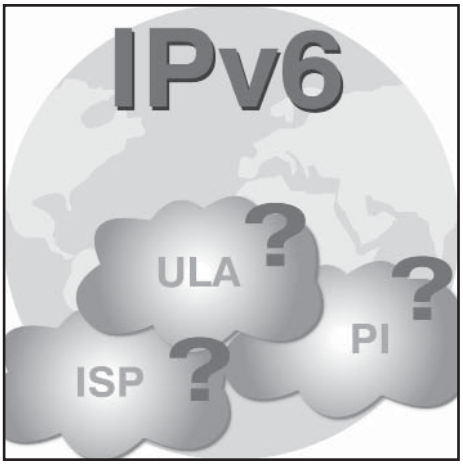
Schwerpunktthema

IPv6 Adresse: die Qual der Wahl

von Markus Schaub

Jeder, der schon einmal eine Umstellung von IP-Adressen durchlebt hat, weiß um den damit verbundenen Horror. Jeder, der schon einmal eine Umstellung von IP-Adressen durchlebt hat, möchte das nie wieder. Darum ist die Frage nach der richtigen Präfix-Wahl bei IPv6 wohl auch die am meisten und emotionalsten geführte Diskussion in unseren Kursen.

"Nicht noch ein Artikel zum Thema IPv6-Adressen" mag sich so mancher jetzt denken. Doch während die meisten Artikel dieses Thema eher technisch angehen, stellt dieser die Fragen nach den Vor- und Nachteilen der verschiedenen Präfixe.



Seien sie nun Unique, Local oder Global. Da die Varianten vielfach eher emotional diskutiert werden, tut es Not, ein wenig Objektivität in die bevorstehenden Entscheidungen zu bringen. Und so mag am Ende des Artikels für so manchen ein überraschendes Ergebnis stehen.

weiter auf Seite 14

Zweitthema

Die Post-PC-Ära und ihre Auswirkungen

von Dr. Behrooz Moayeri, Dr. Simon Hoff, Dominik Zöller

Aktuell wird in den Medien intensiv über das Ende der PC-Ära gesprochen. Die damit gemeinten Entwicklungen haben gravierende Folgen für die IT in Unternehmen. Der vorliegende Beitrag diskutiert diese Entwicklungen in verschiedenen Bereichen, insbesondere in Unified Communications, Netzen und der IT-Sicherheit.

Das Ende der PC-Ära in Zahlen

Drei Jahrzehnte lang haben Menschen die Informationstechnik vor allem mittels PCs genutzt. Anfangs als Gerät für den privaten Gebrauch konzipiert, durchdrang der PC sehr bald die Unternehmens-IT und wurde zum De-facto-Standard für das beruflich genutzte Benutzerendgerät. Es gibt weltweit über eine Milliarde PC-Benutzer. Der PC ist ein Paradebeispiel dafür, wie die IT schon einmal, vor ca. einem Vierteljahrhundert, von der sogenannten „Consumerization“ erfasst wurde.

weiter auf Seite 24

Aktuelle Kongresse

ComConsult IPv6-Forum 2012
ComConsult IT-Sicherheits-Forum 2012

ab Seite 8

Geleit

Corporate Networks 2012: Tendenzen und Herausforderungen

auf Seite 2

Standpunkt

Wenn die Informationssicherheit überreagiert

auf Seite 23

Neues Seminar

Mobile Device Management - Betrieb von mobilen Endgeräte-Flotten

auf Seite 21

Zum Geleit

Corporate Networks 2012: Tendenzen und Herausforderungen

Das Missverhältnis zwischen möglichem Wachstum und notwendiger Vorsicht beim Einsatz finanzieller Mittel ist DER dominante Planungsfaktor für DV und Netze. In einem noch nie dagewesenen Umfang sind Skalierbarkeit und Flexibilität gefragt.

Die Hersteller von DV-Einrichtungen haben nur zum Teil entsprechende Vorsorge getroffen. Der Grad der von einem Hersteller zu erwartenden Innovationen ist davon abhängig, ob er genügend eigene Mittel hat, diese auch zur Produktreife und auf den Markt zu bringen. Prominente Beispiele für Hersteller, die auf einem wirklich beeindruckenden Cash-Vorrat sitzen, sind IBM, Apple, Google und Cisco.

Bedeutung für Unternehmens-DV und Corporate Networks

Die Aufgabe des Planers einer Unternehmens-DV ist es, mit möglichst geringem Kapitaleinsatz eine Struktur maximaler Flexibilität zu schaffen, die beim Anziehen des Geschäftes blitzschnell erweitert werden kann. Genau das bringt es auf den Punkt.

Es hat keinen Sinn, wie in der Vergangenheit oft geschehen, gewaltige Summen für eine DV-Hochrüstung auszugeben, deren Kapazität vielleicht erst in drei oder vier Jahren ausgenutzt wird und erst in fünf oder sechs Jahren an ihre Grenzen stößt. Das war oft gängige Praxis, aber es ist heute weder nötig noch zeitgemäß, diese blockartigen Planungs- und Beschaffungsvorgänge weiter zu betreiben.

Der wesentliche Grund ist, dass sich die Preise für Komponenten nach wie vor im freien Fall befinden. Diese Tendenz ist auch unumkehrbar. Man wird für die gleiche Komponente im Lauf der Zeit immer weniger bezahlen oder für das gleiche Geld immer mehr Leistung bekommen. Das gilt für Speicher genau so wie für Prozessoren und Netzwerk-Komponenten. Sehen wir uns diese Bereiche genauer an.

Speicher: flexible skalierbare Lösungen einschließlich Cloud

Hinsichtlich der Speicher haben sich flexible Strukturen durchgesetzt, die es ermöglichen, Speichersysteme unterschiedlicher Technologien und Kosten pro Byte in einer mehrstufigen Hierarchie einzusetzen, die vermöge eines logischen Überbaus gemeinschaftlich und einheitlich angesprochen werden kann. Die tatsächliche Zuordnung von Datenblöcken zu Speichermedien erfolgt automatisch entlang von QoS-Definitionen für die beabsichtigte Nutzung der Blöcke. Die Technologien reichen von (noch recht teuren) SSDs über schnelle und langsame (SATA)-Platten bis hin zu Bändern. Der einzige Haken ist, dass man sich für einen Hersteller entscheiden muss, denn die Konzepte zur logischen Steuerung sind noch nicht wirklich herstellerübergreifend. Das wird sich auch noch ändern, aber das dauert noch ein paar Jahre.

Mittlerweile wird ein anderes Konzept eine erhebliche Ausbreitung finden: Cloud-Storage. Verschiedene Untersuchungen von ComConsult haben ja in 2011 gezeigt, dass Cloud-Storage heute noch nicht den Reifegrad erreicht hat, den wir für einen wirklich verantwortungsvollen Einsatz im Unternehmensumfeld benötigen. Das wird sich aber schneller ändern als man denkt und der Druck wird aus einer ganz anderen Ecke kommen als man vermutet, nämlich dem Privatbe-

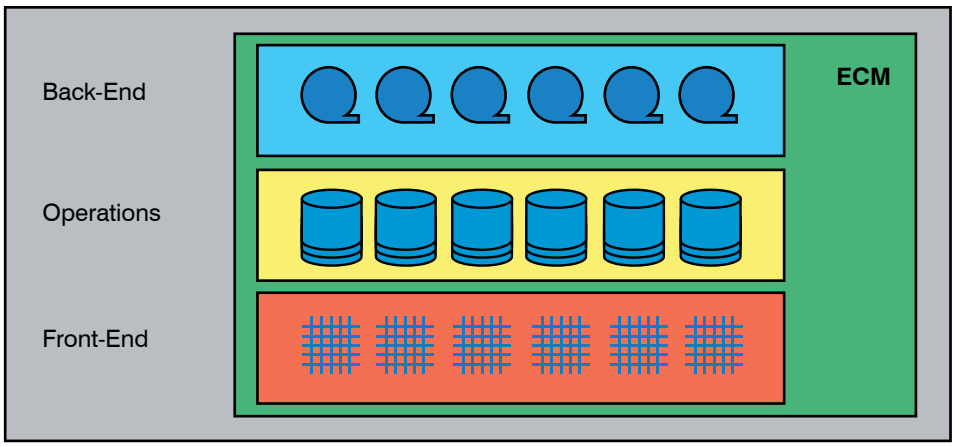


Abbildung 1: Dreistufige Storage-Hierarchie

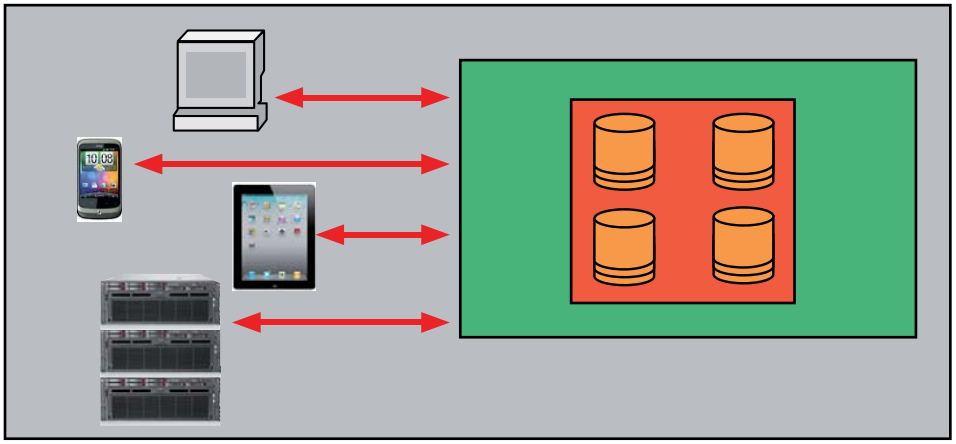


Abbildung 2: Cloud-Storage

reich. Provider und Gerätehersteller bieten schon heute Cloud-Lösungen an, die im Privatbereich durchaus nützlich sein können. Als Beispiele nehmen wir einmal die Telekom-Cloud oder iCloud von Apple.

Beide haben den wesentlichen Vorzug, dass die Nutzung der in der Cloud gespeicherten Daten in weiten Bereichen sowohl unabhängig vom Endgerät (Smartphone, Pad, PC, Notebook, Smart-TV) als auch (heute mit Einschränkungen) unabhängig vom Standort ist. Außerdem sind sie kostenfrei. Für den Betreiber sind die Clouds ein geniales Instrument zur Kundenbindung, denn wenn der Kunde einmal seine ganzen Daten hochgeladen hat, wird er es sich überlegen, den Zugriff darauf durch einen Wechsel zu einem anderen Anbieter zu gefährden.

Ein Unternehmen hätte natürlich auch gerne die gleiche Flexibilität hinsichtlich des Zugriffs auf Daten, zu mindestens in bestimmten Bereichen wie dem Vertrieb. Im Gegensatz zu den Daten einer Privatperson, die selbst entscheiden kann, welche Daten nun in die Cloud dürfen und welche besser nicht, unterliegen Daten von Unternehmen sowohl unternehmenspolitischen als auch gesetzlichen Randbedingungen, die wesentlich höhere Anforderungen an Datenschutz, Integrität und Sicherheit stellen.

Es ist aber nur eine Frage der Zeit bis Provider Angebote auf den Markt bringen, die auch diesen erhöhten Anforderungen Rechnung tragen und vor allem die Sicherheit der Speicherung von Dokumenten vorantreiben.

Ein gutes Muster dafür gibt es schon im Produktivbetrieb: die elektronische Dokumentenverwaltung der Sparkassen. Jeder Besitzer eines Online-Kontos kann seine sämtlichen Kontoauszüge, Wertpapierabrechnungen usf. seit Anfang 2012 darauf umstellen. Der gesicherte Zugriff auf die Dokumente erfolgt im Rahmen des Online Bankings entlang der dort geltenden Sicherheitsmaßnahmen. Es ist eigentlich nur noch ein kleiner Schritt für die Sparkassen Informatik, dieses Angebot in Sinne eines elektronischen Schließfaches zu erweitern, welches für die Ablage elektronischer Dokumente im gleichen Sinn genutzt werden kann wie ein physisches Schließfach für „echte“ Dokumente. Ganz besonders wichtig für den Erfolg derartiger Angebote ist, dass der Kunde einer Sparkasse zu dieser ohnehin ein Vertrauensverhältnis hat, was sich Fremdanbieter ja erst einmal erwerben müssten.

Ein weiteres Produkt, was mir in diesem Zusammenhang als gutes Beispiel aufgefallen ist, ist „Unternehmen online“ der DATEV. Es ist eine gemeinsame Internetbasierende Plattform für den Beleg- und Datenaustausch im Bereich der Finanz- und Lohnbuchführung zwischen Steuerberater und Unternehmen und erlaubt eine revisionssichere Archivierung von digitalen Belegen, elektronischen Rechnungen und Daten. Je nachdem welche DATEV-Produkte sonst noch eingesetzt werden, ist „Unternehmen online“ gratis oder zu einem sehr geringen Monatsbeitrag erhältlich. Dieses Cloud-Angebot kommt von einem Anbieter, der wirklich vertrauenswürdig ist und darüber hinaus ein festes Wissen über die aktuelle Gesetzeslage hat und dies auch umsetzt.

Genau solche Lösungen werden in der Zukunft die Cloud nicht nur zu einem sinnvollen, sondern auch zu einem wirtschaftlich unverzichtbaren Instrument machen. Ich habe weiter unten noch ein schönes Beispiel.

Wie jeder Privatmann wird auch ein Unternehmen Daten haben, die zwar gelagert werden, aber bar jeder Sinnfälligkeit sind. Es kann sich sicher lohnen, diese zu identifizieren und als erste in eine Cloud auszulagern.

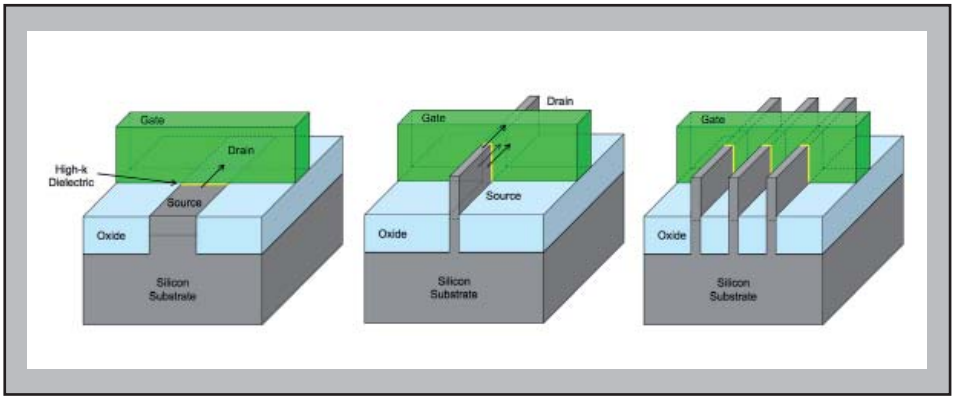


Abbildung 3: Planar-Transistor vs. Tri-Gate Quelle: Intel

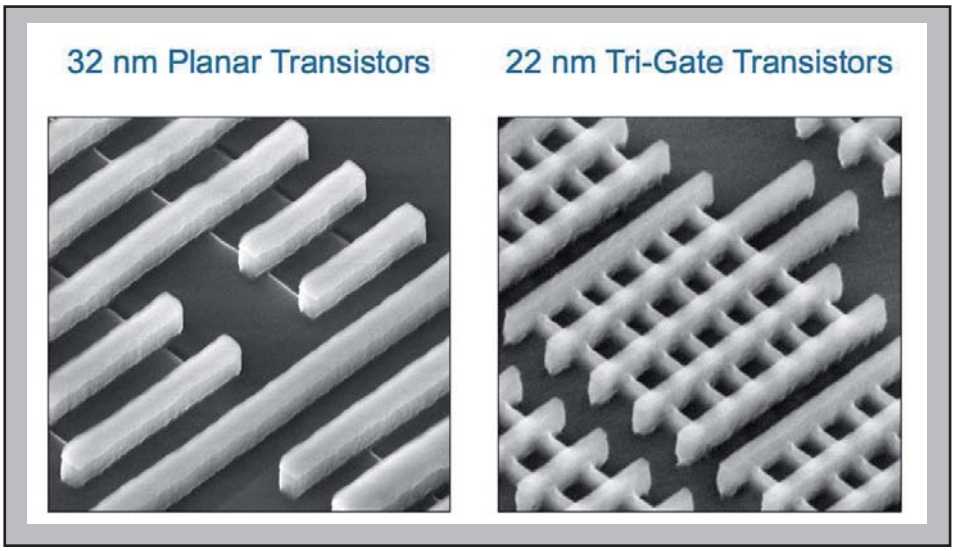


Abbildung 4: Planar-Transistor vs. Tri-Gate: Integrationsdichte Quelle: Intel

Am 02.04.2012 wurde bekannt, dass der Konzern BAT (British American Tobacco) einen „Cloud-Auftrag“ im Umfang von 160 Mio. Euro an die Deutsche Telekom vergeben hat. Über die genauen funktionalen Elemente dieses Auftrags wurde nichts bekannt. BAT ist ein internationaler Konzern mit sehr vielen Niederlassungen. Es ist für BAT offensichtlich günstig, einen transparenten, Standort-unabhängigen Zugriff auf größere Datenmengen zu haben.

Server: x86, Großrechner oder Cloud-Leistung?

Auch auf dem Bereich der Server zeichnet sich eine ähnliche Entwicklung wie bei den Speichern ab. Der Mega-Trend ist auch hier die Flexibilisierung im Hinblick auf eine möglichst enge Anpassung der verfügbaren Leistung an die tatsächlichen Notwendigkeiten.

Corporate Networks 2012: Tendenzen und Herausforderungen

Trotz aller Untergangsgerüchte um Großrechner macht IBM nach wie vor ein stabiles Geschäft mit seinen Hosts, meist eingebettet in Gesamtlösungen. Wer diese Leistung benötigt, weiß das selbst und es gibt hier auch nur wenige Diskussionen.

Bewegter ist der Markt bei den Blade-Systemen und Einzel-Servern. Hier haben sich Konstruktionen auf der Grundlage von x86 eindeutig von den Alternativen absetzen können. IBM und HP sind hier die wichtigsten Lieferanten, aber ein Gewinner des Hangs zu x86 ist auch Cisco. Auf dem US-Markt belegen sie mit den UCS-Systemen den Platz 3 mit immerhin 19% Marktanteil bei den Blade-Systemen. Durch die Neuentwicklungen bei Intel wird Moores Law auch für die nächste Zukunft zementiert. Man kann davon ausgehen, dass sich die Anzahl der in einem Prozessor befindlichen Cores und der damit möglichen Elementarprozesse ungefähr alle 18 Monate verdoppelt.

Durch die Virtualisierungssoftware kann das entsprechend genutzt werden. Das haben wir hier schon so oft diskutiert, dass es nicht mehr weiter ausgeführt werden soll.

Allerdings ergibt sich ein neues Problem: Viele der von Unternehmen eingesetzten Programme können die sich so ergebende Leistung gar nicht mehr richtig nutzen und selbst eine VM im angesprochenen Umfeld könnte deutlich überdimensioniert sein.

Ein weiteres Problem ist, dass die neuen x86-basierendem Prozessorgenerationen zwar bezogen auf ihre Leistung weniger Strom verbrauchen als ihre Vorgänger, dieser Fortschritt aber nicht in der Größenordnung eines wirklichen Durchbruchs liegt.

Deshalb hat sich die Idee entwickelt, Blade-Systeme mit vielen kleinen Prozessoren zu entwickeln, die ursprünglich für den Einsatz in Mobilgeräten gedacht waren und von daher konstruktiv einen wesentlich geringeren Energiebedarf haben. Ein Beispiel dafür wäre die Serie von ARM Holdings, die heute in jedem iPhone oder iPad verbaut wird. Anstelle eines Blade-Systems mit, sagen wir einmal, einem Dutzend Intel-Prozessoren mit ca. 100 Cores und entsprechend vielen VMs tritt ein Blade System mit z.B. 100 oder 200 Mobil-Prozessoren.

HP hat mit dem Projekt Moonshot solche Blade Systeme bereits in der Vorfertigungsstufe. Hier versehen z.Zt. ARM-Prozessoren ihren Dienst, eine Version mit

System-on-Chip mit
4 ARM Cortex A9
Prozessoren pro SoC
1,9 GHz Taktrate
80GigabitCrossbar Switch
SATA Controller

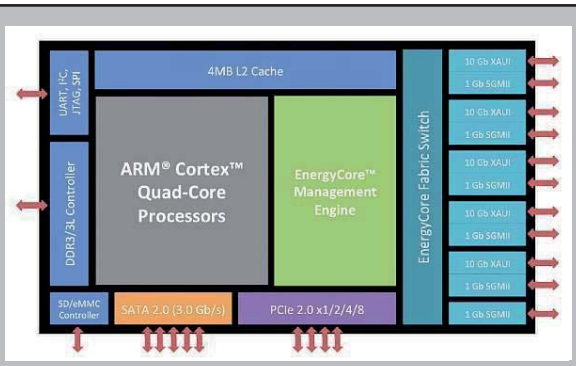


Abbildung 5: Projekt Moonshot: System on Chip Quelle: Hewlett Packard

4 SoCs pro EnergyCard

3x10G pro SoC fürSoC-zu-SoC Kommunikation

2x10G pro SoC Extern = 8x10G proEnergyCard

Abbildung 6: Projekt Moonshot: EnergyCard Quelle: Hewlett Packard

Bis zu 18 EnergyCardspro Sub-Chassis(ohne Platten)

Vier Sub-Chassispro 4HE Chassis

288 SoCs bzw. 1.152Kerne pro Chassis

Abbildung 7: Projekt Moonshot: Sub-Chassis Quelle: Hewlett Packard

mobilen Intel-Prozessoren ist in der Planung. Neben dem dramatisch gesenkten Energieverbrauch gibt es noch eine Reihe weiterer Vorzüge, allen voran der Wegfall der Notwendigkeit einer Virtualisierungssoftware. Bei aller Begeisterung, die wir in den letzten Jahren für die Virtualisierung aufgebracht haben, ist es doch klar geworden, dass dies alles nicht gratis ist und der Preis vor allem in einer erhöhten Komplexität liegt, was man am schnellsten beim Netzwerkanschluss merkt. Obwohl es doch eigentlich das Ziel einer jeden vernünftigen Planung sein sollte, die Komplexität zu senken, fügt die Virtualisierung merkbar Komplexität hinzu. Das wiederum steigert den betrieblichen Aufwand und somit die Kosten.

Sehen wir uns das mal etwas näher an. Basis ist ein Systemchip mit Prozessor, Speicher und einigen Schnittstellen. Auf dem Chip ist auch ein Ethernet-Switch, wie der Autor es schon seit mehreren Jahren prognostiziert.

Vier solcher Chips bilden eine Basis-Baugruppe, die der Hersteller EnergyCard nennt.

Bis zu 18 solcher EnergyCards passen in ein Sub-Chassis. Davon passen wieder vier in ein 4-HE-Chassis, was am Ende bis zu 288 SoCs oder 1152 Kerne ergibt.

Die Vorzüge dieser Konstruktion sind nach Herstellerangaben enorm, siehe Abbildung 8.

Das lassen wir jetzt einfach mal so stehen, denn man kann die Vorzüge der Konstruktion auch anders beschreiben:

Corporate Networks 2012: Tendenzen und Herausforderungen

Prozessoren sehr geringer Leistungsaufnahme bilden zusammen mit der direkt integrierten Kommunikations-Infrastruktur ein Rechnernetz aus über 1000 Knoten in einem einzigen kompakten Gerät. Jeder Prozessor ist z.B. in der Lage, eine der Millionen Apps, wie sie z.B. für die iPads und Smartphones entwickelt wurden, laufen zu lassen. Aufgrund der Struktur können alle Apps sofort mit hoher Leistung und geringer Latenz untereinander kommunizieren. Dies schafft die Grundlage für eine völlig neue Klasse von Anwendungen auf der Grundlage eng kommunizierender Apps. Das beinhaltet natürlich auch die Möglichkeit der Portierung von Grid-Strukturen und anderen HPC-Konstrukten.

Auf eine Perspektive von fünf Jahren könnte das der Anfang vom Ende der Virtualisierungssoftware sein.

Auch bei den Prozessoren kommt man um den Begriff „Cloud“ nicht herum. Der Gedanke, dass sich Unternehmen bedarfsweise Prozessorleistung ausleihen, ist zwar nett, trifft aber in vielen Fällen einfach nicht den Bedarf. Auch hier wird die Entwicklung ganz eindeutig in Richtung angereicherter Services gehen.

Viele wichtigen Hersteller haben im letzten Jahr den Sektor „Cloud“ erheblich aufgerüstet, meist durch Übernahmen. Dafür haben sie sicherlich ihre Gründe. Besonders aufgefallen sind mir zwei Deals, die eine zunächst ungewöhnlich erscheinende Zielrichtung haben.

IBM hat für 440 Mio US$ den Hersteller Demandtec gekauft. Dieser Hersteller hat sich auf Cloud-Analysesoftware spezialisiert. Mit ihr können die Informationsflüsse in einer Cloud analysiert und in einem zweiten Schritt auch zielgerichtet gesteuert werden. Einsatzfelder wären z.B. Analyse von Cloud-basierenden Kundendaten für Marketingzwecke aber auch die Überwachung der allgemeinen Leistungsfähigkeit von Cloud-Diensten. Das passt sehr gut in das projektorientierte Geschäft von IBM.

Spannend vor allem für viele deutsche Kunden könnte sein, dass SAP für kräftige 3,4 Mrd. US$ die Fa. SuccessFactors übernommen hat. SuccessFactors ist ein Spezialist für Mietsoftware. Mit Hilfe von SuccessFactors könne SAP neben dem angestammten Verkauf von Software-Lizenzen zur Unternehmenssteuerung künftig auch jede Software zur Miete anbieten und auf Mobil-Computern zur Verfügung stellen. Denn SuccessFactors hat viel Kompetenz bei der Programmierung von Cloud-Anwendungen.

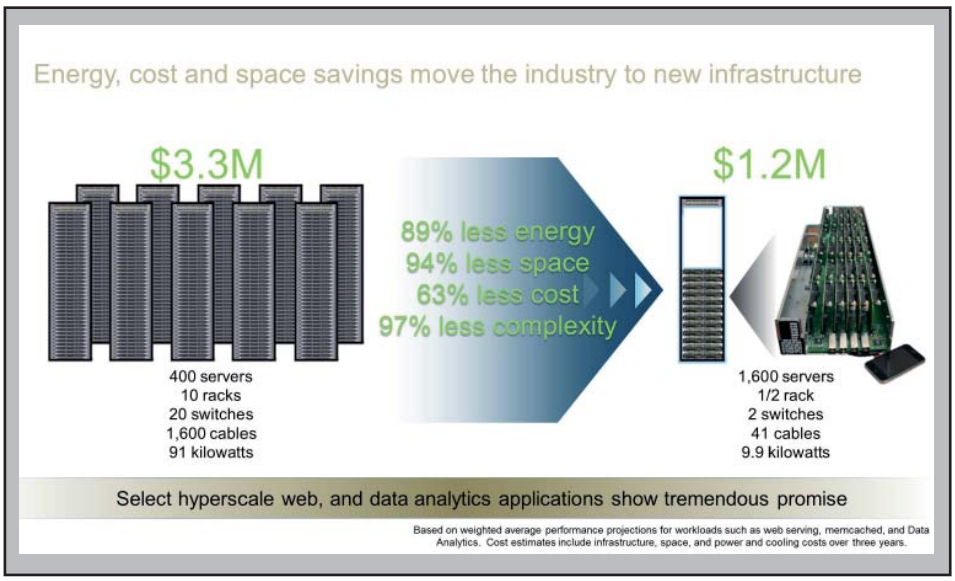


Abbildung 8: Breakthrough Savings and Simplicity Quelle: Hewlett Packard

SAP hat sich bisher eher langsam in den Zukunftsmarkt Mietsoftware vorgearbeitet. Erst Mitte vergangenen Jahres kam die Mittelstands-Software Business by Design auf den Markt, die den Weg in den Milliarden-Markt für internetbasierende Software-Modelle ebnen sollte. Für die mit hohem finanziellen Aufwand entwickelte Software, die zur Miete über das Internet abgeboten wird, will SAP am Ende dieses Jahres 1000 Kunden haben. Zum Vergleich: Im klassischen Geschäft zählt SAP derzeit gut 175.000 Kunden, die Software-Lizenzen von den Walldorfern kaufen. Gemeinsam mit der Software-Schmiede SuccessFactors und ihren knapp 1500 Mitarbeitern soll nun der Durchbruch gelingen. Bisher zählen die Kalifornier rund 3500 Kunden weltweit, die für die Nutzung von Personal-Management-Software über das Internet zahlen. 2012 soll der Umsatz auf gut 330 Millionen Dollar steigen.

Apps für Smartphones und Tablets sind ein Renner. Es gibt keinen technischen Grund, nicht auch größere „Apps“ für größere Server ebenso erfolgreich zu vermarkten.

Marktforscher erwarten, dass in den kommenden Jahren immer mehr Software über das Internet genutzt und gemietet wird. Das Marktvolumen könne sich nach Forrester in den kommenden neun Jahren auf rund 240 Milliarden Dollar versechsfachen.

Und von da aus ist es nicht mehr weit zu

einem von SAP oder einem Dritten betriebenen Cloud-Service, der die gesamte Verarbeitung der Unternehmensdaten übernimmt.

Die zentrale Frage angesichts derartiger Entwicklungen, die sich Unternehmen und Organisationen auf eine Perspektive von 5 – 10 Jahren stellen müssen, lautet:

Ist ein eigenes großes RZ eigentlich noch nötig und wirtschaftlich?

Natürlich ist die Antwort auf diese Frage nicht ja oder nein, sondern sehr differenziert. Ein sicherer Trend ist aber die Auslagerung von Standard-Aufgaben.

Netzwerke: Welche Leistung für wen?

Die Zeiten, in denen die Netzwerkleistung nach dem Gießkannenprinzip verteilt werden konnte, sind endgültig vorbei. Spannend ist also vor allem die Frage, an welcher Stelle welche Leistung benötigt wird und was das bedeutet.

Der in 2012 alles dominierende Begriff in diesem Zusammenhang ist nicht etwa das Terabit-Ethernet, sondern vielmehr: BYOD! Wie schon in meinem Geleit zum November-Insider dargestellt, ist der Druck von der Seite der Mitarbeiter, die von zu Hause gewohnte Leichtigkeit und Vielfalt des Endgerätespektrums auch für ihre Arbeit zur Verfügung zu haben, massiv mit täglich steigender Tendenz. Ein modernes Unternehmen kann es sich nicht leisten, die Mitarbeiter weiterhin an fest installierte Kästen zu binden.

Damit fallen natürlich diese ganzen schon länger suspekten Verkabelungsstrategien in sich zusammen. Sie stammen aus der Mitte des letzten Jahrhunderts und wir sollten sie auch wieder dahin zurückschicken. Auffällig ist nur, dass die notwendige Leistung pro Endgerät sozusagen über Nacht anders beurteilt wird als vor zwei Jahren. Damals musste es mindestens ein Gigabit pro Endgerät sein, heute sind die meisten User plötzlich mit geshartem 802.11n zufrieden.

Das liegt schlicht an der Tatsache, dass die zunächst für die Smartphones entwickelten Apps mit der Ressource Übertragungsweg wesentlich sparsamer umgehen. Hersteller wie Apple wollten ja erreichen, dass man die wesentlichen Segnungen des Gerätes auch dann nutzen kann, wenn man nur einen 3G-Mobilfunk-Kanal zur Verfügung hat. Jedes Mal, wenn man Safari aufmacht, fragt das iPhone verzweifelt nach einem WLAN. Gibt es aber keins, macht es auch so weiter. Und es gibt dann eben optimierte Apps, die auch damit gut umgehen können. Ich

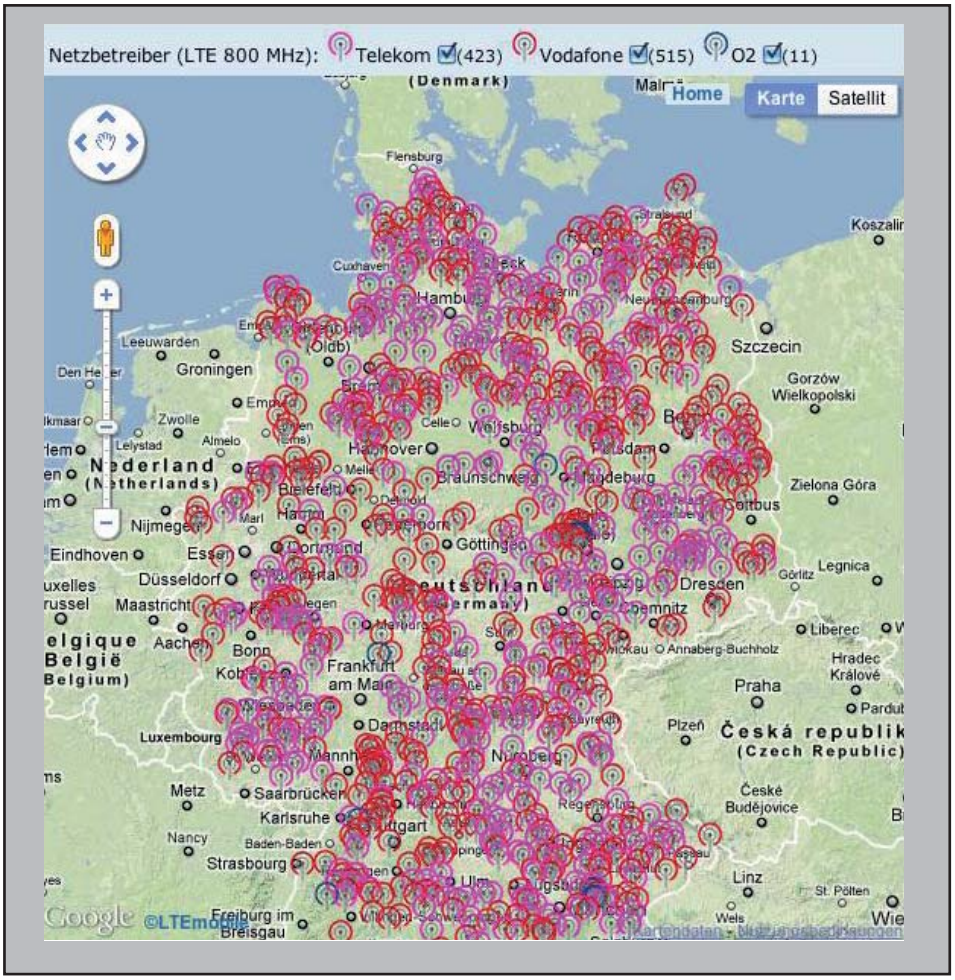


Abbildung 9: LTE in Deutschland

nenne als Beispiel einmal die Sparkassen-App, eine der beliebtesten Apps in Deutschland.

Das ist jetzt aber nicht für die Ewigkeit zementiert und der Bandbreitenbedarf von Smartphones und Pads wird schnell steigen. Spätestens 2014 wird es mehr mobile als stationäre Endgeräte geben.

Unternehmen bleibt momentan nichts anderes übrig, als flächendeckend 802.11n-Netze zu installieren, obwohl man eigentlich jetzt schon die Container zur Entsorgung der 802.11n-APs aufstellen kann. Die Nachfolgegeneration 802.11ac wird schon in 2012 kommen, 802.11ad in der Breite eher erst 2015. Dann bekommt man Gigabits, aber immer noch in einem shared Modus.

Obwohl WiFi-WLANs den überwiegenden Teil des IP-Verkehrs tragen werden, ist auch die 3G-Nachfolgegeneration LTE wesentlicher Bestandteil der zukünftigen Versorgung. Hier hat sich Ende 2011 einiges entschieden und der Konkurrent WiMax ist weitest gehend aus dem Rennen. Mit der Einführung des iPad 3 im ersten Quartal 2012 haben AT&T, Verizon und Sprint LTE-Services etabliert. Das iPhone 5 wird ebenfalls 4G-LTE unterstützen, daher bauen die Provider ihre Backbones z.Zt. kräftig aus. Qualcomm ist der primäre Lieferant für die LTE-Chips in iPad und iPhone. T-Mobile (USA) investiert ebenfalls Milliarden in den Ausbau der LTE-Infrastruktur.

Die von ltemobile.de angefertigte Karte über die Verfügbarkeit von LTE in Deutschland ist schon erfreulich bunt. Die Deutsche Telekom, Vodafone und O2 waren viel fleißiger als man vielleicht denkt und haben den Ausbau vor allem in bisher eher strukturschwachen Gebieten erheblich vorangetrieben. Call & Surf Comfort via Funk (LTE / HSPA) kostet Ende 2011 bei der Deutschen Telekom 39,95 Euro pro Monat mit bis zu 7,2 Mbps beim Surfen.

Unter der Annahme, dass sich mit einem Provider angesichts des Wettbewerbs und eines größeren Mengengerüstes auch ein günstigerer Preis von sagen wir einmal 20,00 Euro/Monat aushandeln

lässt, stellt sich natürlich die Frage, ob es für ein Unternehmen überhaupt noch irgendeinen wirtschaftlichen Vorteil bringt, eine eigenständige, flächendeckende (!), hinreichend leistungsfähige WLAN-Installation vorzunehmen.

Das wird bestimmt ein ganz spannendes Thema in 2012, vor allem dann, wenn man BYOD ernst nimmt und diese Bereiche verknüpft. Denn ein Provider-Dienst zeichnet sich in jedem Falle dadurch aus, dass die Geräte und damit die von ihnen ausgehenden logischen Verbindungen in jedem Fall deutlich voneinander getrennt sind, was ein wesentliches Merkmal für die Sicherheit ist. Bei WLANs muss man das ja erst einmal selbst basteln. Und die Kosten für WLANs sind ja bei den Access Points noch lange nicht zu Ende. Spätestens ab 802.11ad benötigt man eine 10-GbE-Verbindung vom AP zum nächsten Switch, entsprechend ausgestattete Switchports und den Rest des vollen Programms.

Ein Unternehmen sollte sich schon einmal mit dieser Frage auseinandersetzen, bevor die ersten Mitarbeiter spätestens im Herbst kommen und sich darüber beschweren, dass die iPhone 5 nicht recht funktionieren.

Was ist mit den anderen Netzwerk-Bereichen im Unternehmen?

2011 war das Jahr, in dem uns praktisch alle Hersteller mit neuen Strategien zu RZ-Netzen überhäuft haben. Abgesehen davon, dass nur zwei Hersteller wirklich in Stückzahl liefern konnten, was sie da so schön angekündigt haben, war die Reaktion der möglichen Betreiber eher verhalten. Zu viele Details sind noch unklar und mit Schaudern habe ich von einem sehr großen Systemhaus hören müssen, dass die Diskussion um Themen wie z.B. FCoE bei den Kunden jetzt erst langsam losgeht. 40- und 100-GbE brauchen zunächst auch nur wenige, genauso wie eine ultra geringe Latenz. In 2012 werden sich alle diese Dinge erst einmal setzen und wirklich bahnbrechende Neuheiten sind nicht zu erwarten.

Das gilt auch für die unternehmenseigenen Backbones. Vor einem massiven Ausbau sollte zunächst einmal die Frage gestellt werden, was man wirklich benötigt. Sollte sich in 2012 herausstellen, dass man die Benutzer mittelfristig mit LTE abfackelt, benötigt man keinen Terabit-fähigen Backbone.

Konsequenzen

Die Aufgabe eines Planers für die DV eines Unternehmens ist es, mit möglichst geringem Kapitaleinsatz eine Struktur maximaler Flexibilität zu schaffen, die beim Anziehen des Geschäftes blitzschnell erweitert werden kann.

Die Ausführungen der letzten Absätze sollten gezeigt haben, wie sich die Technologie weiterentwickelt, um genau dies zu ermöglichen.

Ein wirklich schwerwiegender Fehler wäre, jetzt sozusagen panisch auf Vorrat völlig überdimensionierte Speicher-, Rechen- und Netzwerkleistung einzukaufen. Ein großer Teil dieser Investitionen würde sich niemals rentieren, genau wie die in der Größenordnung von Lichtjahren verlegten teuren Kat.7-Kabel.

Vielmehr gilt es, einen Plan zu entwickeln, der, von einer hinreichend leistungsfähigen Startmenge an Equipment ausgehend, ein in der Zukunft notwendiges Leistungswachstum durch die einfache Hinzufügung von entsprechenden Komponenten ermöglicht. Dabei ist hinsichtlich der Netze eine strenge Standardisierung erforderlich, die aber durch den Ansatz des skalierbaren Ethernet in IEEE 802.11ab ausreichend unterstützt wird. Bei Speichern wird man sich für einen Hersteller entscheiden müssen.

Im Rahmen jeder Erweiterungsplanung sollte allerdings auch die Frage behandelt werden, ob, und wenn ja, wie die Auslagerung von Aufgaben in eine Cloud-Lösung möglich, sinnvoll und kostengünstig ist. In 2012 wird der Markt beginnen, eine erhebliche Anzahl wie an den Beispielen besprochene, funktional angereicherte Cloud-Lösungen hervorzubringen. Da passt sicher nicht immer alles, aber es ist wichtig, frühzeitig wahrzunehmen, dass hier ein wichtiger Zweig für Entscheidungen entsteht, den es vorher noch nicht gab.

Zur Erklärung sei noch eine Analogie gestattet. Social Networks wie Facebook standen noch vor nicht allzu langer Zeit im Ruf, vom Datenschutz her ausgesprochen bedenkliche Spaßvehikel für gelangweilte Teenager zu sein. Die Datenschutzbedenken gibt es immer noch, aber mit Hilfe der Social Networks wurden 2011 nicht nur vergleichsweise harmlose falsche Doktoren entlarvt, sondern im arabischen Frühling bösartige Diktatoren gleich reihenweise gekippt. Das hätten diese sich auch niemals so vorgestellt.

Cloud Computing wird zusammen mit den neuen Endgeräten eine ähnliche Kraft entwickeln und mittelfristig bisher als fundamental angenommene Erkenntnisse über die Gestaltung unternehmensweiter DV genauso wegwischen wie bösartige Diktatoren.

Aktueller Kongress

ComConsult IPv6-Forum 2012

21.05. - 23.05.12 in Düsseldorf

Die ComConsult Akademie veranstaltet vom 21.05. - 23.05.12 ihr "ComConsult IPv6-Forum 2012" in Düsseldorf.

Die gute Nachricht zuerst: Auch die 6. Version von IP kann Pakete rund um die Welt transportieren. Darüber hinaus ändert sich eine ganze Menge. IPv6 ist nicht IPv4 mit anderen Mitteln. Wer mit IPv6 beginnen möchte, und sei es nur ein Pilotprojekt mit wenigen Teilnehmern, muss bereits Entscheidungen treffen, die weitreichende Folgen haben, da sie sich nicht ohne weiteres rückgängig machen lassen.

Überspitzt formuliert, könnte man sagen Version 6 und 4 haben so viel miteinander gemeinsam wie der Benz Patent-Motorwagen Nummer 1 mit dem Mercedes F1 W03: Beide haben einen Verbrennungsmotor und keinen Kofferraum.

Um im Bild zu bleiben: So wie die Erfindung des KFZ über die letzten Jahrzehnte Auswirkungen auf den Straßenbau hatte, so beeinflusste IP die Infrastruktur der Netze und umgekehrt. Aus Klingeldrähten wurden Datenautobahnen, aus einer manuell gepflegten Hosttabelle ein hoch dynamisches, dezentrales Namenssystem und aus einer Technik für Nerds eine Massenbewegung.

Diese Veränderungen hatten aber auch Rückwirkungen auf das Protokoll selbst. Bei der ursprünglichen Entwicklung von IP war es völlig in Ordnung, dass Namenstabellen und IP-Adressen manuell gemanaged wurden. Man konnte davon ausgehen, dass stets ein versierter Techniker vor Ort war, um Änderungen durchzuführen und neue Systeme einzurichten.

Dank des omnipräsenten Internets jedoch ist IP mittlerweile in vielen Haushalten und Hosentaschen zu finden. Die Nutzer erwarten, ein Telefon im Discounter nebenan kaufen und sofort lossurfen zu können. Dass das heute wirklich möglich ist, liegt daran, dass IP hochgradig flexibel ist. Jedoch wurde nie das Protokoll selbst geändert, sondern es wurden Zusatzmechanismen entwickelt, die gleichsam an IP drangeflanscht wurden: DHCP, DNS und OSPF um nur einige zu nennen. Viele dieser Mechanismen haben sich bewährt. Andere wirken bis auf den heutigen Tag gekünstelt, weil es keine „externen“ Zusatzfeatures von IP sind, sondern vielmehr integrale Bestandteile des Protokolls sein sollten. Prominentestes Beispiel dafür ist wohl DHCP. Es ist weder Bestandteil des eigentlichen Internet Protokolls, noch ist es überhaupt ein eigenständiges „echtes“ Protokoll. Vielmehr handelt es sich um ein aufgebohrtes und bis zur Unkenntlichkeit verändertes BOOTP, dessen protokollarischen Ballast es aber immer noch mit sich herum schleppt.

Als man die Entwicklung von IPv6 startete, wollte man den unnötigen Ballast abwerfen und wichtige Funktionen „in dem Protokoll“ integrieren. Damit ist IPv6 weit mehr als nur eine Vervierfachung der Adresslänge:

- Autokonfiguration und Neighbor Discovery werden integrale Protokollbestandteile
- Broadcasts wurden abgeschafft
- ICMP ist funktionaler Bestandteil und kein nettes Ad-On mehr
- NAT von Version 6 nach Version 6 wird es nicht mehr geben
- Unique Local Adressen sind mehr als nur der Nachfolger der private IPv4 Adressen
- und viele mehr

Wer sich gut mit IPv4 auskennt, hat damit zwar eine gute Startposition, jedoch das Rennen noch lange nicht gewonnen. Vieles kann schief gehen. Jeder, der IPv6 einführen will, muss sich mit den neuen Techniken, Adresstypen, Konfigurationen und Fallstricken auseinandersetzen.

Das ComConsult IPv6-Forum 2012 greift die wesentlichen Aspekte für die Einführung und den Betrieb von IPv6 strukturiert auf und zeigt den optimalen Weg nach IPv6. Im Mittelpunkt des Kongresses stehen dabei folgende Top-Themen, die für alle Planer und Betreiber von Netzwerken wichtig sind: IPv6-Design, Sicherheit, Migration, Betrieb und aktueller Stand von Komponenten und Anwendungen. Top-Berater und versierte Anwender berichten von ihren Erfahrungen und stellen sich den Fragen der Teilnehmer.

Das ComConsult IPv6-Forum ist ein Muss für alle Betreiber und Planer von Netzwerken, Endgeräten, Servern, Speichersystemen und Applikationen im Netzwerk. Versäumen Sie nicht, sich rechtzeitig einen Platz auf dieser herausragenden Veranstaltung zu sichern.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

ComConsult IPv6-Forum 2012

Ich buche den Kongress
ComConsult IPv6-Forum 2012
☐ vom 21.05. - 23.05.12 in Düsseldorf
zum Preis € 2.090,-- netto

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 12

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

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

Programmübersicht - ComConsult IPv6-Forum 2012

Montag, den 21.05.2012

Themenblock: Vision
9:30 bis 10:45 Uhr
IPv6-Vorbereitung: Warum, wann und wie?
- Warum kein Weg an IPv6 vorbei geht
- Welche Entscheidungen jetzt schon getroffen werden müssen
- Chancen und Risiken von IPv6
- Erfahrungen eines Umstellungs-Projektes

Markus Schaub, ComConsult Research Ltd.

10:45 bis 11:15 Uhr Kaffeepause

11:15 bis 12:30 Uhr
IPv6 Design & Infrastruktur
- Struktur und Umgang mit den neuen IPv6 Adressen
- Was sich bei Routing und VRRP geändert hat
- Einsatz von Infrastrukturdiensten: DNS und/oder DHCP
- Wie sieht ein modernes Netzdesign mit IPv6 aus?
  - Access-Bereich / Campus / Data Center / IPv6 und Layer-2 Konzepte wie VLANs, DCB, AVB
- Designvarianten I - Dual-Stack: Funktionsweise, Vorteile, Nachteile
- Designvarianten II – Tunneling: Funktionsweise, Vorteile, Nachteile
- Grundsätzliche Designvarianten III – Translation: Funktionsweise, Vorteile, Nachteile • Was müssen IPv6-fähige Layer-2- und Layer-3-Netzkomponenten können?

Dipl.-Inform. Petra Borowka-Gatzweiler, Unternehmensberatung Netzwerke UBN

12:30 bis 14:00 Uhr Mittagspause

14:00 bis 14:45 Uhr
IPv6@Bosch
- Warten oder starten - wann ist der richtige Zeitpunkt für ein Großunternehmen, mit IPv6 zu beginnen? Und warum?
- IPv6 betrifft die gesamte IT und alle Netzwerk-Funktionen - wo starten?
- Wie bindet man ein IPv6-Projekt erfolgreich in die Organisation ein?
- Welche Erfahrungen hat Bosch nach einem Jahr IPv6? Wo gab es Schwierigkeiten, was funktionierte auf Anhieb, was ist anders als bei IPv4?
- Ausblick: Wie geht es weiter mit IPv6 @ Bosch?

Anja Moog-Lölkes, Robert Bosch GmbH

14:45 bis 15:15 Uhr Kaffeepause

Themenblock: Sicherheit
15:15 bis 16:15 Uhr
Sicherheitsrisiken in IPv6
- Mehr Sicherheit durch IPv6?
- Der Reifezustand der IPv6 Implementationen
- Risiken automatischer Konfiguration
- Herausforderungen für den Firewall Einsatz
- Beschränkter Nutzen von Sicherheitsfunktionalitäten

Marc Heuse, Consultant

16:20 bis 17:20 Uhr
Sicherheit - IP Sicherheit: Neue Konzepte
- Welche Beiträge durch Netzkomponenten zur IPv6-Sicherheit absehbar sind, notwendige Sicherheitsbeiträge vernetzter Geräte („IPv6-Hosts“) im Zusammenspiel mit den Netzkomponenten
- Was sich im Bereich der Firewalls ändert
- Was man durch Auswahl aus Konfigurationsalternativen zur Sicherheit beisteuern kann
- Visionen vs. Produktverfügbarkeit - IPv6-Readiness bzgl. Sicherheit?

Dipl.-Inform. Oliver Flüs, ComConsult Beratung und Planung GmbH

ab 18:00 Uhr - Get Together

Dienstag, den 22.05.2012

Themenblock: Migration
9:00 bis 10:15 Uhr
Migrationstechniken
- Welche Phasen ein IPv6 Migrationsprojekt hat
- Wie die Entscheidung für ein Adresskonzept vorbereitet wird
- Wann das Netzwerk auf IPv6 migriert werden sollte
- Typische Einsatzszenarien während der Migration
- Wann Dual Stack zum Einsatz kommen sollte
- Wann Tunneling zum Einsatz kommen sollte
- Wann Translation zum Einsatz kommen sollte
- Überprüfung von IPv6 Readiness – Was bringt eine Zertifizierung?

Dipl.-Inform. Petra Borowka-Gatzweiler, Unternehmensberatung Netzwerke UBN

10:15 bis 10:45 Uhr Kaffeepause

10:45 bis 11:30 Uhr
IP Address Management für IPv6 - Welche Lösung passt ?
- Warum bei IPv6 eine zentrale Adressverwaltung unverzichtbar ist
- Welche Produkte es am Markt gibt
- Welchen Funktionsumfang alle Produkte gemeinsam haben
- Was die konzeptionellen Unterschiede der Lösungen sind
- Wie weit die IPv6- Integration in welchem Tool ist

Dipl.-Ing. Thomas Erhardt, n3k Informatik GmbH

11:35 bis 12:20 Uhr
Das Management erwartet für alle Fälle ein fertiges IPv6-Konzept, was nun?
- Worauf es bei der Bestandserfassung ankommt
- Was in der Zwischenzeit zu tun ist
- Wie mit nicht IPv6-fähigen Anwendungen umzugehen ist
- Was ab sofort zu beachten ist

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

12:20 bis 14:00 Uhr Mittagspause

14:00 bis 14:45 Uhr
Anwendervortrag: Projektierung eines IPv6 Projektes

Themenblock: Aktueller Stand
14:50 bis 15:35 Uhr
Provider

15:35 bis 16:05 Uhr Kaffeepause

16:05 bis 16:50 Uhr
Software/VoIP

Mittwoch, den 23.05.2012

Themenblock: Betrieb
9:00 bis 9:45 Uhr
Cisco - IPv6 Strategie und innovative Migrations-Technik mit LISP
- IPv6 Strategie / IPv6 Zertifizierungen / IPv6 Roadmap
- Migration mit LISP

Gerd Pflüger, Cisco Systems GmbH

9:50 bis 10:50 Uhr
Betrieb - Einbindung von Endgeräten
- Der „Werkzeugkasten“ im Überblick - IPv6-Mechanismen mit Relevanz für den Endgerätebereich
- Der Endgerätebereich - betrieblich realistische Zielsetzungen in verschiedenen Phasen der IPv6-Einführung
- Dual Stack/ Dual Layer: ob, wann und wie lange zur Einbindung von Endgeräten? - bekannte Stolperfallen für den Endgerätebetrieb
- Theorie und Praxis - Konzeptideen und Produktunterstützung

Dipl.-Inform. Oliver Flüs, ComConsult Beratung und Planung GmbH

10:50 bis 11:20 Uhr Kaffeepause

11:20 bis 12:30 Uhr
Mobilität, Smartphones & Tablets
- IPv6 für Anwendungen und zum Transport - zwei unterschiedliche Blickrichtungen
- IPv6 in Wireless LANs
- IPv6 in Mobilfunknetzen
- IPv6-Fähigkeit typischer mobiler Endgeräte
- Wann kommt die IPv6-fähige App?
- Ergebnisse unserer Praxistests

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

12:30 bis 14:00 Uhr Mittagspause

14:00 bis 14:45 Uhr
Trouble-Shooting in IPv6-Umgebungen
- Protokoll-Know-how - Voraussetzung für erfolgreichen IPv6-Betrieb
- Protokollanalysatoren und IPv6
- Typische Fallstricke bei IPv6
- Beispiele aus der Fehlersuche-Praxis

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

14:50 bis 15:30 Uhr
Fazit & Ausblick
- Was waren die wichtigsten neuen Erkenntnisse aus den Vorträgen
- Welche Schlussfolgerungen können daraus gezogen werden
- Welche Handlungsweisen lassen sich daraus ableiten

Markus Schaub, ComConsult Research Ltd.

15:30 Uhr Ende der Veranstaltung

Der Veranstalter behält sich Änderungen im Programm vor!

Aktueller Kongress

ComConsult IT-Sicherheits-Forum 2012

18.06. - 19.06.12 in Düsseldorf

Frühbucherphase bis zum 15.04.2012

Die ComConsult Akademie veranstaltet vom 18.06. - 19.06.12 Düsseldorf ihr "ComConsult IT-Sicherheits-Forum 2012" in Düsseldorf.

Im Moment zeichnen sich massive Veränderungen in der IT ab, zu denen die Informationssicherheit nicht nur eine Risikobewertung vornehmen, sondern sich selbst neu erfinden muss:

- Die Nutzung mobiler Endgeräte wie Smartphones und Tablets in Unternehmen und Behörden steigt exponentiell. Der traditionelle PC hat immer mehr ausgedient.
- Innovation in der IT findet im Consumer-Bereich statt und damit drängen Consumer-Techniken automatisch verstärkt in die Enterprise-IT.
- Mit Bring Your Own Device (BYOD) materialisiert sich der Wunsch private Endgeräte im Unternehmensnetz für Zugriff und Verarbeitung von dienstlichen Daten einzusetzen.
- Die Vision „IT als Dienst aus der Steckdose“, d.h. Unternehmensdaten und -anwendungen sind überall und mit jedem Endgerät verfügbar, wird immer ernster diskutiert.
- Die Zukunft der Kommunikation mit Clients ist drahtlos, d.h. WLAN, UMTS/LTE und Co. werden das klassische Kabel für die Client-Anbindung zur Nischenlösung machen.
- Unified Communications (UC) hat nicht nur die klassische TK aussterben lassen, UC verändert auch die IT. Traditionelle Zonenarchitekturen in RZ und Campusnetzen werden durch UC ad absurdum geführt.
- Consumerization dehnt sich auch auf den Anwendungsbereich aus. Bei sozialen Netzen, Skype und Co. geht es längst nicht mehr um die private Nutzung aus der dienstlichen IT heraus, sondern um die Nutzung für Unternehmenszwecke.
- Die eigene IT-Infrastruktur wird zunehmend durch externe Parteien betrieben, letztendlich ist Information das einzige Eigentum was noch übrig bleibt.
- Hosting von Rechenleistungen, Anwendungen und Speicher ist inzwischen so normal geworden, dass wir gar nicht gemerkt haben, dass Cloud Computing - anfänglich für den Enterprise-Bereich mehr belächelt als tatsächlich genutzt - die strategische Ausrichtung für IT-Dienstleistungen geworden ist.
- Das Data Center in a Box ist keine Vision mehr. Verschiedenste hochgradig dynamische komplett virtuelle IT-Infrastrukturen (d.h. Clients, Server, Netz und Storage), die gemeinsam auf einer physischen Hardware laufen, sind längst Realität.

Diese Entwicklungen in der IT haben direkte Konsequenzen für die Informationssicherheit:

- Die Integration von Smartphones und Tablets erfordert ein Mobile Device Management (MDM), das nicht monolithisch auf einen Systemtyp bzw. Hersteller ausgerichtet ist (z.B. Blackberry), sondern alle relevanten Systeme von iOS bis Android unterstützt.
- Für die IT-Sicherheit waren strikte Standardisierung und Kontrolle immer Kerninstrumente. IT-Sicherheit und Anarchie durch Consumerization der IT und BYOD kommen daher scheinbar einer Quadratur des Kreises gleich. Hier sind zunächst spezielle Techniken aus den Bereichen Mobile Device Management (MDM), Server-based Computing und Virtualisierung erforderlich, um private und dienstliche Daten zu trennen.
- Für BYOD sind außerdem spezifische Netzwerkkonzepte erforderlich, die letztendlich in eine Mandantenfähigkeit und die Notwendigkeit einer Netzzugangskontrolle (Network Access Control, NAC) münden.
- Mit BYOD gestattet man den Anschluss eines Fremdgeräts an die eigene Infrastruktur. Im WLAN ist dies mit vergleichsweise überschaubarem Aufwand verbunden. Möchte man ein solches Konzept auch auf das kabelbasierte LAN ausdehnen, wird man zur Trennung von Spreu von Weizen auch im kabelbasierten LAN oft um den Einsatz von IEEE 802.1X nicht herum kommen, was im Gegensatz zu WLAN im LAN ein höchstkomplexes Vorhaben ist.
- Mandantenfähigkeit erfordert stets die sichere Trennung der Informationen der Mandanten. Die traditionelle Methode der Informationssicherheit einer möglichst physikalischen Trennung auf Ebene des Netzes und der Endgeräte ist nicht mehr zeitgemäß. Virtualisierung und UC erfordern ein Umdenken in Richtung logischer Trennung und insbesondere in Richtung kryptographischer Techniken.
- Auf Zonenkonzepte auf Basis von Firewalls wird man trotzdem nicht verzichten können. Im Gegenteil: Zonenkonzepte in RZ und Campus werden zu einem normalen Gestaltungsinstrument. Schwerpunkte sind dabei die logische Trennung von Zonen in Virtualisierungsplattform, Netz und im Storage-Bereich.

ComConsult IT-Sicherheits-Forum 2012

- Die sichere Administration der Infrastruktur durch externe Dienstleister stellt besondere Ansprüche. Es sind Konzepte nötig, die zielgerichtet nur erlaubte Zugriffe gestatten und verhindern, dass ein Administrator ausgehend von dem administrierten System unberechtigt auf andere Systeme zugreift. Dies ist angesichts der Rechte eines Administrators technisch höchst anspruchsvoll und erfordert seinerseits spezifische Zonenkonzepte, in denen unter anderem Lösungen zur Entkopplung externer Zugriffe, zur Protokollierung von Administrationssitzungen und zur Nutzer- und Anwendungs-basierten Berechtigung von Zugriffen zum Einsatz kommen.

- Für den Nutzer einer virtuellen IT im Zeitalter des Cloud Computing muss sich die Informationssicherheit auf ihren Namen besinnen und Sicherheitsmaß-nahmen müssen sich auf die Informationen selbst konzentrieren. Kernelemente sind nicht nur die Zusicherung von Vertraulichkeit und Authentizität durch Verschlüsselungstechniken sondern immer mehr die Nachvollziehbarkeit von Änderungen an Daten (Revisionsfähigkeit) und die Kontrolle von unerwünschtem Abfluss von Daten, d.h. letztendlich Klassifikation von Daten in Verbindung mit Data Loss Prevention.

- Die klassischen Methoden und Prozesse der Informationssicherheit sind zu schwerfällig für eine IT, die maximale Mobilität für den Zugriff auf Information und für die Information selbst als Credo erhoben hat. Wir können nicht mehr für jede neue Anwendung aufwendige Sicherheitsbetrachtungen machen, wenn die Zeit zwischen Anforderungsanalyse und Produktivsetzung immer kürzer wird.

Aus diesen Gründen konzentriert sich das IT-Sicherheits-Forum 2012 auf folgende Themenbereiche:

- Sicherheit von Smartphones und Tablets, insbesondere iOS und Android

- Mobile Device Management (MDM): Techniken und Produkte

- Bring Your Own Device (BYOD): Techniken, Werkzeuge und Sicherheitskonzepte

- NAC mit IEEE 802.1X: Architekturen, Fallstricke und Projekterfahrungen

- Mandantenfähigkeit und Zonenkonzepte in RZ und Campus: Netz- und Firewall-Architekturen, Server- und SAN/NAS-Anbindung

- Sichere Netze: Risiken und Konzepte für UMTS/LTE und WLAN, Sorgenkind IPv6
- Sicherer Betrieb durch externe Dienstleister: Protokollierung und Berechtigung

- Cloud Computing: Sicherer Nutzung von Clouds, Aufbau sicherer private Clouds und Anforderungen an sichere Public Clouds

- Konzentration auf Information: Datenklassifikation, Data Loss Prevention und Revisionsfähigkeit

- Moderne Prozesse der Informationssicherheit: Integration in die schnelllebige IT

Wie auch in den Vorjahren greift das IT-Sicherheits-Forum 2012 die aktuellsten Entwicklungen im Bereich der Informationssicherheit auf. Das Forum ist wie folgt strukturiert:

- Vorträge mit Top-Referenten und Erfahrungsberichten aus der Praxis

- Neueste Forschungsergebnisse der ComConsult für zukunftssichere Investitionen

- Begleitende Ausstellung in Kombination mit einem Vortragswettbewerb zur Präsentation der besten Projekte und Ideen in der Veranstaltung

- Get Togehter am ersten Tag

Das ComConsult IT-Sicherheits-Forum 2012 ist die zentrale IT-Sicherheits-Veranstaltung des Jahres 2012. Sie ist für jeden Entscheider, IT-Sicherheitsbeauftragten, Planer und Betreiber in diesem Bereich ein absolutes Muss. Hier trifft sich die Branche.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
ComConsult
IT-Sicherheits-Forum 2012

Ich buche den Kongress
ComConsult IT-Sicherheits-Forum 2012
☐ vom 18.06. - 19.06.12 in Düsseldorf
zum Preis € 1.690,-- netto*

*Preis gültig bis zum 15.04.2012 -
dann regulärer Preis von € 1.890,-- netto

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 12

im Hotel nikko Düsseldorf

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

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

Programmübersicht - ComConsult IT-Sicherheits-Forum 2012

Montag, den 18.06.2012

9:30 - 10:15 Uhr
Keynote: Das Ende der PC-Ära und die Konsequenzen für die Informationssicherheit
- Aussterben des klassischen Fat Client
- Schwindende Vertrauenswürdigkeit des Intranet
- Smart Phones, Tablets und Bring Your Own Device: Umgang mit unsicheren Endgeräten und Auswirkung auf Netz und Zonenarchitekturen
- Künftige Rolle von NAC und mandantenfähigen Campusnetzen
- Server-based Computing, Virtualisierung und Cloud Computing verändern die IT-Sicherheit
- Paradigmenwechsel: Maßnahmen auf Ebene der Daten selbst sind notwendig

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

10:15 - 11:00 Uhr
Smartphones und Tablets: Risiken und Sicherheitsmaßnahmen
- Sicherheitsalptraum Smartphone & Tablet – Wie gefährlich sind mobile Endgeräte?
- Plattformen und Betriebssysteme im Vergleich – Ist Sicherheit à la Blackberry mit Android und iOS möglich?
- Bekannte Sicherheitslücken und Bedrohungen am Beispiel von Android und iOS
- Härtung mobiler Plattformen – Bordmittel und Zusatzprodukte

Dominik Zöller, ComConsult Beratung und Planung GmbH

11:00 - 11:30 Uhr Kaffeepause

11:30 - 12:15 Uhr
Mobile Device Management (MDM): Techniken und Produkte
- Von der Sicherheitsrichtlinie bis zur Inventarisierung - Was leistet Mobile Device Management?
- Von ActiveSync bis Afaria – MDM-Lösungen im Überblick
- Plattformabhängigkeit von MDM-Lösungen – Einschränkungen von Android und iOS
- Was muss MDM in Zeiten von BYOD leisten?

Dominik Zöller, ComConsult Beratung und Planung GmbH

12:15 - 13:00 Uhr
Bring Your Own Device (BYOD) oder die Quadratur des Kreises
- Sicherer Zugriff auf Infrastruktur und Daten mit Sandboxing, Server-based Computing und Virtualisierung
- Reichen Sandboxing und Verschlüsselung für BYOD aus?
- Notwendigkeit von Mobile Device Management
- Server-based Computing und Smartphone-Virtualisierung
- Die Grenzen der Technik: Risiken von BYOD
- Nicht trivial: WLAN-Architekturen für BYOD
- BYOD im kabelbasierten LAN: Mission impossible?

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

13:00 - 14:15 Uhr Mittagspause

14:15 - 15:00 Uhr
Rechtliche Aspekte von BYOD und IT-Consumerization
- Grenzen der Kontrolle eigener Geräte des Benutzers
- Netzverantwortlichkeit des TK-Betreibers nach der TKG-Novelle 2012
- Beschäftigtendatenschutzgesetz - Neuregelung von Standortbestimmung und Stichprobenkontrolle
- Tunnelbau und rechtliche Grenzen der Maulwurfsbekämpfung
- Datensicherheit und Urheberrecht bei „gerooteten“oder „gejailbreakten“ Geräten

Ulrich Emmert, e/s/b Rechtsanwälte

15:00 - 15:45 Uhr
Network Access Control: Architekturen, Fallstricke und Projekterfahrungen
- Die Verschiebung von NAC als reine Security Lösung hin zur Netzwerkautomatisierung
- Multiple Mandanten, wie kommen die Nutzer ins richtige VPN?
- IEEE 802.1X und Co.: Welche Techniken zum Einsatz kommen, wo die Probleme liegen und wie in der Praxis damit umgegangen werden kann
- NAC als Basis für BYOD Projekte
- Die Anatomie eines typischen NAC Projektes
- Betrieb einer NAC-Lösung
- Projektbeispiele aus den Bereich Healthcare, Automotive, Government, Forschung im deutschsprachigen Raum

Markus Nispel, Enterasys Networks GmbH

15:45 - 16:15 Uhr Kaffeepause

16:15 - 16:45 Uhr
Einführung und Betrieb von IEEE 802.1X bei der IKB Data
- Herausforderung IEEE 802.1X für PCs,Thin Clients und Drucker
- Autorisierung mit ACLs
- Lessons learned: Typische Fehlersituation und wie damit umgegangen worden ist
- Standortübergreifende Einführung und Betrieb der NAC-Lösung

Alex Bruckhaus, Ulrich Wolf, IKB Data GmbH

16:45 - 17:30 Uhr
Ausstellerpräsentationen

ab 18:00 Uhr Get Together

Dienstag, den 19.06.2012

9:00 - 9:45 Uhr
Server-based Computing, Virtualisierung und Cloud Computing in der Analyse
- Kapselung von Daten und Anwendungen im RZ mit Server-based Computing und Desktop Virtualisierung
- Gefährdungen durch Zentralisierung von Clients
- Sind neue Konzepte beispielsweise für den Virenschutz erforderlich?
- Sicherheitsarchitekturen für Private Clouds
- Rolle von Public Clouds für die Enterprise IT
- Anforderungen an sichere Public Clouds

Dr. Behooz Moayeri, ComConsult Beratung und Planung GmbH

9:45 - 10:30 Uhr
Mandantenfähigkeit und Zonenkonzepte in RZ und Campus
- Mandantenfähige Campus-Netze: Techniken und deren Praxistauglichkeit
- Brauchen wir angesichts Server-based Computing und Cloud Computing noch Sicherheitsmaßnahmen im Intranet?
- Zonen- und Firewall-Architekturen im RZ
- Server-Anbindung und Load Balancing
- Zwiebelschalen-Modelle im Widerspruch zu Domänen-orientierten Zonenkonzepten à la Microsoft

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

10:30 - 11:00 Uhr Kaffeepause

11:00 - 11:45 Uhr
Web-Anwendungen, die Lösung aller Probleme?
- Die Architektur von Web-Anwendungen
- Neue Gefahren dank Apps
- Offline Web-Applikationen dank HTML5: ein Alptraum für die Datensicherheit?
- Server, Endgeräte, Smartphones und Tablets: wie sieht ein umfassendes Sicherheitskonzept aus?

Markus Schaub, ComConsult Research Ltd.

11:45 - 12:30 Uhr
Konzentration auf Information: Datenklassifikation, Data Loss Prevention und Next Generation Firewalls
- Next Generation Firewalls: Anwendungs - und User-zentrische Filterung der Kommunikation
- Methoden und Werkzeuge zur Klassifikation von Dokumenten und Daten
- Techniken zur Erkennung und Verhinderung eines Datenabflusses
- Data Loss Prevention: Host-basierte und Netz-basierte Systeme im Vergleich
- DRM und Co: Einsatz kryptographischer Mechanismen zur Kontrolle von Ausbreitung und Nutzung der Daten

N.N.

12:30 - 13:45 Uhr Mittagspause

13:45 - 14:30 Uhr
Sicherer Betrieb von Zonenarchitekturen
- Terminal Server als Jump Host: Möglichkeiten und Grenzen
- Virtualisierungstechniken zur sicheren Entkopplung administrativer Zugriffe
- Zonen für die Administration und Überwachung: Firewall-Infation droht
- SIEM: Sondermülldeponie oder sinnvolles Instrument des Security Incident Management?
- Kurzschluss in SAN und NAS vermeiden

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

14:30 - 15:15 Uhr
Nachvollziehbarkeit in derAdministration
- Typische Anforderungen und Herausforderungen
- Protokollierung von administrativen Zugriffen auf IT-Systeme
- Verfügbare Techniken und ihre Grenzen
- Marktüberblick und Auswahlkriterien

Marco Lorenz, cirosec GmbH

Ende der Veranstaltung 15:30 Uhr

Der Veranstalter behält sich Änderungen im Programm vor!

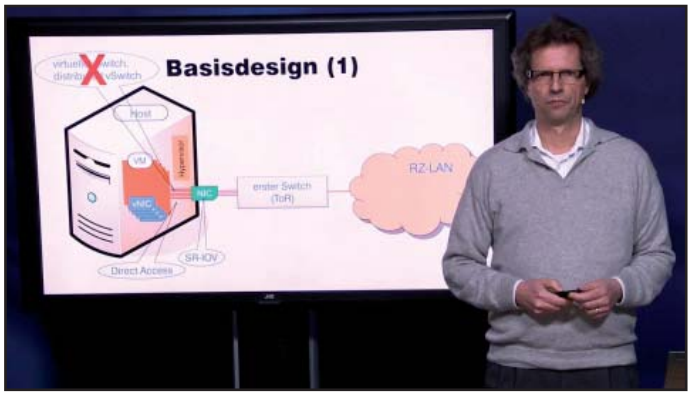
ComConsult-Study.tv

Aktuelle Neuerscheinungen bei ComConsult-Study.tv

Themenbereich: Analyse und Strategie
Bring Your Own Device
Referent: **Dr. Simon Hoff**
Zeit: 00:40:22
Einzelpreis: 59,00 € netto Im Abo: kostenlos

Bring Your Own Device wirkt wie die Quadratur des Kreises: zufriedene Benutzer mit modernsten Applikationen bei gleichzeitig sinkenden IT-Kosten für das Unternehmen. Dr. Hoff analysiert in diesem hochaktuellen Video welche Rahmenbedingungen mit BYOD einher gehen. Die zentrale Frage ist: ist es möglich, Sicherheit für Unternehmens-Daten und Applikationen zu schaffen ohne die Privatnutzung des Benutzers einzuschränken?

Themenbereich: Netzwerke
Seminar: Anbindung virtueller Maschinen
Referent: **Dipl.-Math. Cornelius Höchel-Winter**
Zeit: 00:54:14 gesamt
Einzelpreis: 59,00 € netto Im Abo: kostenlos

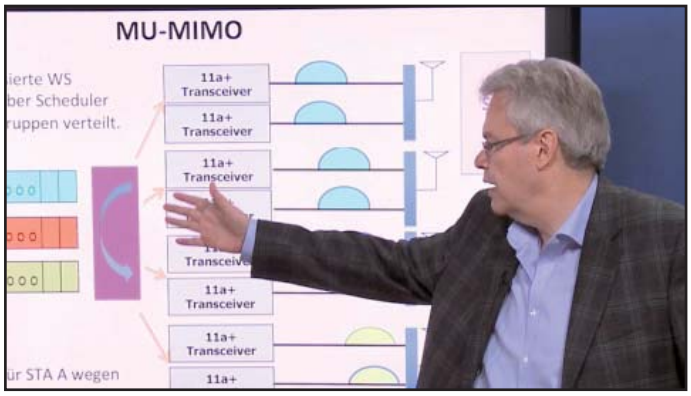


Ist Ihre Infrastruktur den Anforderungen moderner Virtualisierungslösungen gewachsen? Von diversen Spielarten virtueller Switche über Direct Access und SR-IOV bis hin zu den aktuellen Standardisierungsbestrebungen der IEEE stehen eine ganze Reihe Technologien zur Anbindung virtueller Server im Rechenzentrum zur Verfügung. Nicht alle sind beliebig kombinierbar und einige haben Auswirkungen tief in das Design des RZ-Netzes.

Themenbereich: Besser Präsentieren
Seminar: Besser und erfolgreich Präsentieren
Referent: **Lars Sudmann**
Zeit: 02:59:35 gesamt
Einzelpreis: 59,00 € netto Im Abo: kostenlos

Es gibt sie tatsächlich: leicht umsetzbare Empfehlungen, um (noch) mehr Erfolg mit Präsentationen zu haben. Dies gilt für jedes Level an Können, vom Anfänger bis zum Profi. Dabei haben sich die Konzepte für erfolgreiche Präsentationen in den letzten Jahren deutlich verändert. Neue Erkenntnisse aus der Psychologie in Kombination mit neuen technischen Möglichkeiten bilden den Rahmen für erfolgreiche Präsentationen. Und: es kann jeder davon profitieren.

Themenbereich: Netzwerke
Das neue WLAN IEEE 802.11ac: was bringt es?
Referent: **Dr. Franz-Joachim Kauffels**
Zeit: 00:41:51
Einzelpreis: 59,00 € netto Im Abo: kostenlos



Mit der starken Zunahme mobiler Teilnehmer ist das bisherige WLAN nach IEEE 802.11n am Ende. Zwei neue Standards kämpfen um die Gunst des Kunden. Speziell IEEE 802.11ac verspricht 7 Gbit/s zum Preis von 11n. Lernen Sie in diesem Video was der neue Standard IEEE 802.11ac für Sie bedeutet und welche Auswirkung er auf aktuelle Planungen hat.

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

Schwerpunkthema

IPv6-Adresse: die Qual der Wahl

Fortsetzung von Seite 1

Markus Schaub ist seit 2009 Leiter von ComConsult-Study.tv. Er verfügt über umfangreiche Berufserfahrung in den Bereichen Netzwerken und VoIP und ist seit mehr als 13 Jahren bei ComConsult beschäftigt. Seine Schwerpunkte liegen im Netzwerk-Design, IP-Infrastrukturdiensten und SIP, zu denen er viele Vorträge auf Kongressen hielt, erfolgreich Seminare durchführte und zahlreiche Veröffentlichungen schrieb.

Bei der Auswahl des Adresstyps gibt es einige Aspekte zu beachten:

- **Wegfall von NAT**
  Dass NAT von IPv6 nach IPv6 nicht mehr möglich sein wird, hat zur Folge, dass private Adressen wie bei IPv4 nicht mehr existieren. Das hat Konsequenzen für das Design von DMZs: Für jede Anwendung, die eine Kommunikation zwischen internem Netz und dem Internet voraussetzt, werden künftig applikationsspezifische Gateways benötigt. Ein schlichtes Austauschen der IP-Adresse im IP-Header ist nicht mehr möglich.

- **Sicherheit**
  Private IP-Adressen werden nicht nur aus Gründen der Adressknappheit, sondern auch der Sicherheit wegen genutzt. Ein Wechsel zu IPv6 sollte hier keine neuen Sicherheitslöcher öffnen.

- **Zukunftssicherheit**
  Ein Renumbering der internen IP Adressen macht keinen Spaß. Und wenn man sich die IPv6-Adressen ansieht, beschleicht einen das Gefühl, dass es noch weniger Spaß machen wird als bei Version 4. Wenn man sich heute für eine Adressvariante entscheidet, möchte man sicher sein, dass diese sehr lange genutzt werden kann.

- **Skalierbarkeit**
  Ein IP-Design muss so angelegt sein, dass genügend Reserven vorhanden sind, den Bedarf für sehr lange Zeit zu decken, ohne dass es substantiell geändert werden muss. An jedem Standort, für jedes Gebäude, auf jeder Etage müssen genügend „freie“ Netze vorhanden sein, um künftigen Techniken bei Bedarf zur Verfügung gestellt zu werden, so wie das in der Vergangenheit für WLAN- und VoIP-Netze notwendig war.

Die weitaus größere Anzahl von IPv6-Netzen sollte es eigentlich ermöglichen, zumindest die beiden letzten Punkte einfach zu erreichen. Trotzdem muss man beide bei der Planung immer im Hinterkopf haben, da bereits Planungen gemacht wurden, die entweder so verschwenderisch waren, dass die zugewiesenen IPv6 Netze nicht ausreichten oder so knapp, dass die Skalierbarkeit nicht gegeben war. Ein gesundes Augenmaß ist hier gefragt!

Wie viele Netze einem zur Verfügung stehen und ob in jedem Fall ALGs oder Proxies für den Übergang ins Internet notwendig sind, ist davon abhängig, für welche Art von Netzwerkadresse man sich entscheidet.

Adressen

Bei IPv4 gab es zwei „legale“ und eine halbseidene[1] Möglichkeit für interne IP Adressen. Legal nutzte man entweder zugewiesene, global gültige IP-Adressen oder private, die im RFC 1918 festgelegt sind.

Situationsanalyse

Unternehmensintern sind die privaten Adressen wohl am meisten verbreitet. Für die Kommunikation mit Partnern und dem Internet wurde NAT genutzt. Dieses Vorgehen hat einige Vor- und Nachteile:

Vorteile

- **Adressknappheit**
  IPv4 Adressen sind schon lange Mangelware. Kaum ein Unternehmen verfügt über ausreichend Adressen, um alle internen Systeme mit öffentlichen IP Adressen zu versorgen. Und wenn doch sind sie so knapp bemessen, dass ein sauberes IP-Design kaum möglich ist.

  Das 10er-Netz mit seinen rund 65.000 Class-C-Netzen bzw. fast 17 Mio. Adressen bot einen komfortablen Ausweg.

- **Keine Umnummerierung bei Providerwechsel**
  Nur wenige haben das Glück, öffentliche IP-Adressen nutzen zu können, die sie nicht von ihrem Provider zugewiesen bekommen haben. Das bedeutet jedoch, dass ein Providerwechsel zwangsläufig zu einer Umnummerierung aller Systeme mit öffentlichen IP Adressen führt.

  Die Nutzung privater IP-Adressen im internen Netz reduziert den Aufwand auf wenige Server in der DMZ, Internet-Gateways und Firewalls.

- **Sicherheit**
  Häufig angeführt wird der Sicherheitsaspekt der Sicherheit privater IP Adressen: da sie im Internet nicht geroutet werden, können interne Systeme nicht ohne weiteres adressiert und direkt angegriffen werden.

- **Usertracking**
  Da NAT die „echte“ IP-Adresse verbirgt, kann ein User / ein Gerät nicht identifiziert werden und damit kann er sich anonym im Internet bewegen ... so ein weit verbreiteter Aberglaube.

- **Plug’n’Play**
  Hersteller von Heimroutern können DHCP-Server für die Verteilung von privaten IP-Adressen auf ihren Geräten vorkonfigurieren. Dadurch sind „Plug’n’Play“-Heimnetze für den Massenmarkt möglich.

Nachteile

- **Doppelte IP-Adressen**
  Jeder der schon mal eine Firmenfusion mitgemacht hat, kennt das Problem: Doppelte IP-Adressen. Nahezu jedes Unternehmen nutzt das 10er-Netz und

[1] Einige haben irgendwelche IP-Adressen genutzt und darauf vertraut, dass es NAT schon irgendwie richten oder ein Anschluss an das öffentliche IP-Netz nie notwendig würde. Dieses Vorgehen wird gelegentlich als „illegale IP-Adressnutzung“ bezeichnet und im Folgenden nicht weiter betrachtet.

fängt bei den Subnetzen bei 1 an zu zählen. Damit sind bei Fusionen oft in beiden Unternehmen dieselben IP Netze vergeben. Die Probleme sind vorprogrammiert, ein schnelles Ändern der IP-Adressen ist häufig nicht möglich. Als Lösungen stehen nur Krücken zur Verfügung, die die Betreiber der notwendigen NAT+DNS-Konstruktionen in die Verzweiflung treiben.

- **Eingeschränkte Kommunikation**
  Nicht erst seit VoIP, Telekonferenzing und Instant Messaging gibt es Anwendungen, die eine Any-to-Any Kommunikation voraussetzen. Also die Erreichbarkeit interner Geräte von außen. Mit NAT sind diese Anforderungen entweder nur schwer oder gar nicht umzusetzen. Meist bleibt nur der Ausweg Gateways zu nutzen, die jedoch stets anwendungsspezifisch sind. Beispiele dafür wären Session Border Controller und Application Layer Gateways bei VoIP.

- **Scheinsicherheit**
  Kein ernst zu nehmender Sicherheitsexperte behauptet, dass NAT ein Sicherheitsmechanismus ist. Skype & Co demonstrieren eindrucksvoll, wie man eine Firewall durchtunneln kann und mit Teredo hat Microsoft gleich eine Möglichkeit geschaffen, ein ganzes Layer-3-Protokoll – nämlich IPv6 – und alles was es transportiert durch NAT-Gateway in beide Richtungen zu tunneln[2].

- **Usertracking**
  Jeder der Google oder Amazon nutzt, sollte sich keine Sorgen darüber machen, ob man ihn über seine IP-Adresse identifizieren kann. Es gibt weitaus elegantere Möglichkeiten[3].

Unique Local

Die Schöpfer von IPv6 wollten die aus ihrer Sicht wesentlichen Vorteile beider Welten zusammenbringen: kein Renummerierung weder bei Providerwechsel noch bei Firmenfusionen. Dazu wurden die Unique Local Adressen, kurz ULA, erfunden. Das von RFC 4193 dafür vorgesehen Präfix ist fc00::/7, also alles was mit „fc“ oder „fd“ beginnt. Wie die privaten Adressen von IPv4 werden auch diese Adressen im Internet nicht geroutet. Formal bauen sie sich wie in Abbildung 1 dargestellt auf.

Für jedes ULA-Präfix gibt es somit 2^{16} Subnetze, also 65.536, was der Anzahl von Class-C-Netzen im 10er-Netz entspricht. Wer damit nicht auskommt, kann weitere ULA Präfixe generieren.

ULAs soll es in zwei Ausprägungen geben:

1. **Global administriert: fc00::/8**
   Die Idee ist es, analog zu den Registrars für öffentliche geroutete IP-Adressen: auch ULAs zentral und somit weltweit eindeutig zu vergeben. Damit könnte sichergestellt werden, dass bei Fusionen oder bei der Kommunikation mit Partnern keine Adressen doppelt vergeben sind.

   So charmant diese Idee auch ist, sie ist Science Fiction: Weder gibt es einen solche zentrale Registratur noch gibt es einen RFC, der sich damit befasst. Der letzte entsprechende Internet-Draft ist am 10.07.2010 ausgelaufen und wurde nicht erneuert.

2. **Zufällig erzeugt: fd00::/8**
   Statt eines Zentralregisters setzt die zweite Variante von ULAs auf einen Zufallsalgorithmus. Man hofft, dass 2^{40}, also rund eine Billionen ULA Präfixe ausreichen, um es hinreichend unwahrscheinlich zu machen, dass eines mehrfach erzeugt wird. Und selbst wenn das passieren sollte, kommt es erst dann zu Problemen, wenn diese beiden Netze/Unternehmen auch direkt miteinander kommunizieren wollen. Sprich per VPN oder direkter Leitung.

Bit	1-7	8	9-48	49-64
Bedeutung	Prefix	L	Globale ID	Subnetz ID
Vorgaben	fc00::/7	1	Pseudo Zufällig	Lokales Design
Beispiel	fdea:		f4b4:f8f5:	f100

Abbildung 1: Aufbau, Bedeutung und Beispiel von ULAs

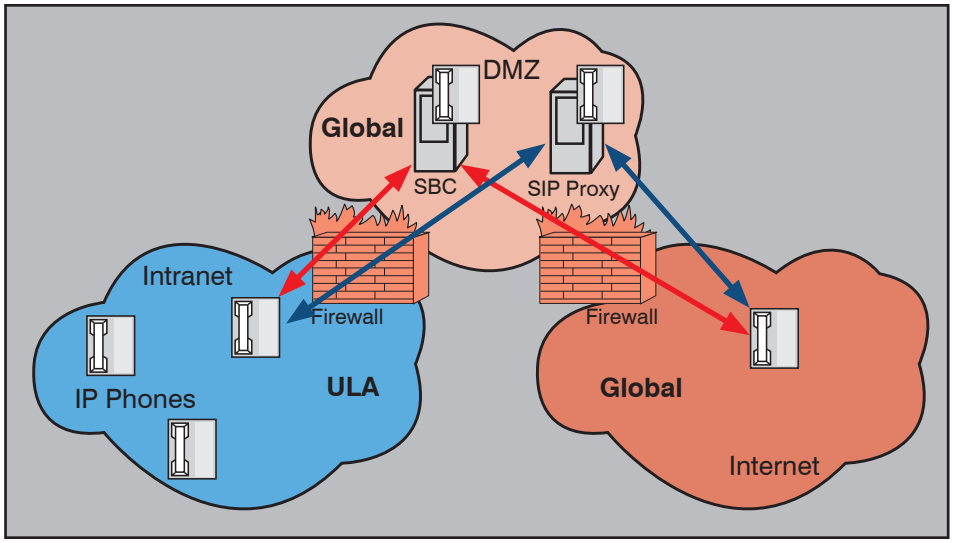


Abbildung 2: Internetzugang mit ULA

Fassen wir zusammen, was mit ULAs erreicht wurde und was nicht:

Pro

- **Firmenfusion und Providerwechsel**
  In beiden Fällen müssen internen Systemen keine neuen Präfixe zugewiesen werden.

- **Netzdesign**
  Es stehen ausreichend Präfixe für ein skalierbares und zukunftssicheres IP-Design zur Verfügung

- **Sicherheit**
  Durch den Wegfall von NAT müssen bei IPv6 applikationsspezifische ALGs bzw. Proxys eingesetzt werden. Ein Durchtunneln mittels NAT Traversal der Firewall ist somit nicht mehr so ohne weiteres möglich.

Contra

- **Sicherheit**
  ULAs bringen allerdings wenig echte Sicherheit, da bereits jetzt viele Tunnel auf HTTP als Trägerprotokoll basieren. Trotzdem bietet ein Proxy auch in diesen Fällen mehr Sicherheit als eine „NAT Firewal“. (vgl. Abbildung 2)

- **Anwendungen, für die keine Proxys / ALGs existieren**
  Es gibt Anwendungen, für die keine ALGs bzw. Proxys existieren.

- **Künftige Entwicklung von P2P-Anwendungen**
  IPv6 ermöglicht es – wieder –, P2P-Anwendungen ohne NAT Traversal Mechanismen zu entwickeln. Auch wenn wir

[2] Der Erfinder des Wortes „NAT-Firewall“ sollte zunächst einen hoch dotierten Marketing-Preis bekommen und anschließend auf eine einsame Insel ohne Internet verbannt werden.
[3] Wer es nicht glaubt, kann es selbst prüfen: https://panopticlick.eff.org

uns heute noch nicht vorstellen können, was das sein wird: Sie werden kommen. Mit ULAs verhindert man deren Einsatz. In Zeiten von Unified Communications, SIP und globaler Erreichbarkeit sollte man sich gut überlegen, sich von diesen Entwicklungen von vornherein auszuschließen.

Globale Adressen

Globale Adressen werden im Internet geroutet. Anders als bei IPv4 ist dafür bislang nur ein kleiner Teil reserviert. Konkret handelt es sich um das Präfix 2000::/3, also alles von 2000:: bis 3fff::. Das sind 2^{61} Präfixe, also rund 2 Trillionen; umgerechnet fast 330 Millionen pro Person. Diese Präfixe sind in verschiedene Bereich aufgeteilt, wie die Vergabe an Provider oder spezielle Tunnelmechanismen bspw. 6to4.

Als Unternehmen hat man zwei Möglichkeiten an öffentliche IP-Adressen zu kommen: Entweder bekommt man sie aus dem Adresspool des eigenen Providers oder man beantragt eine „provider-independent address“ – eine Provider-unabhängige Adresse, kurz „PI“ genannt.

Route Aggregation

Die einfachste Methode, an ein IPv6 Präfix zu kommen, ist, es von seinem Provider zu bekommen. Zudem ist das gleichzeitig die präferierte Methode von

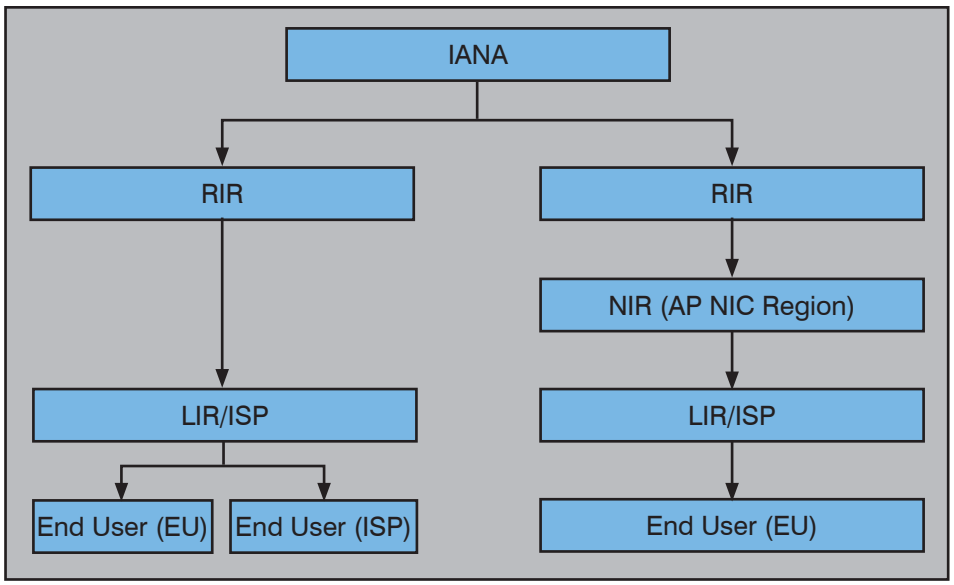


Abbildung 3: Organisationsstruktur der IP-Präfix-Zuteilung

Standardisierern und Verwaltern des Internets. Und dafür gibt es einen einfachen Grund: aggregierbare Routen und damit kurze Routingtabellen im Internet.

Abbildung 3 zeigt die Organisationsstruktur der IP-Präfix-Zuteilung für IPv6-Adressen: alle Adressen gehen vom IANA aus. Das IANA verteilt große, zusammenhängende Präfixe an die Regionalen Internet Registrare (RIR). Diese wiederum geben zusammenhängende Blöcke aus ihren Pools an die Lokalen Internet Registrare (LIR). Das können Provider sein, aber auch sehr große Unternehmen oder Behörden. Die End-User wiederum erhalten ihre Präfixe aus dem Bereich ihres LIRs.

Ziel dieser Vergabepolitik ist es, eine Struktur zu schaffen, die aggregierbare Routen ermöglicht.

Abbildung 4 zeigt den beabsichtigen Aggregierungsprozess anhand des Beispieles von ComConsult Research:

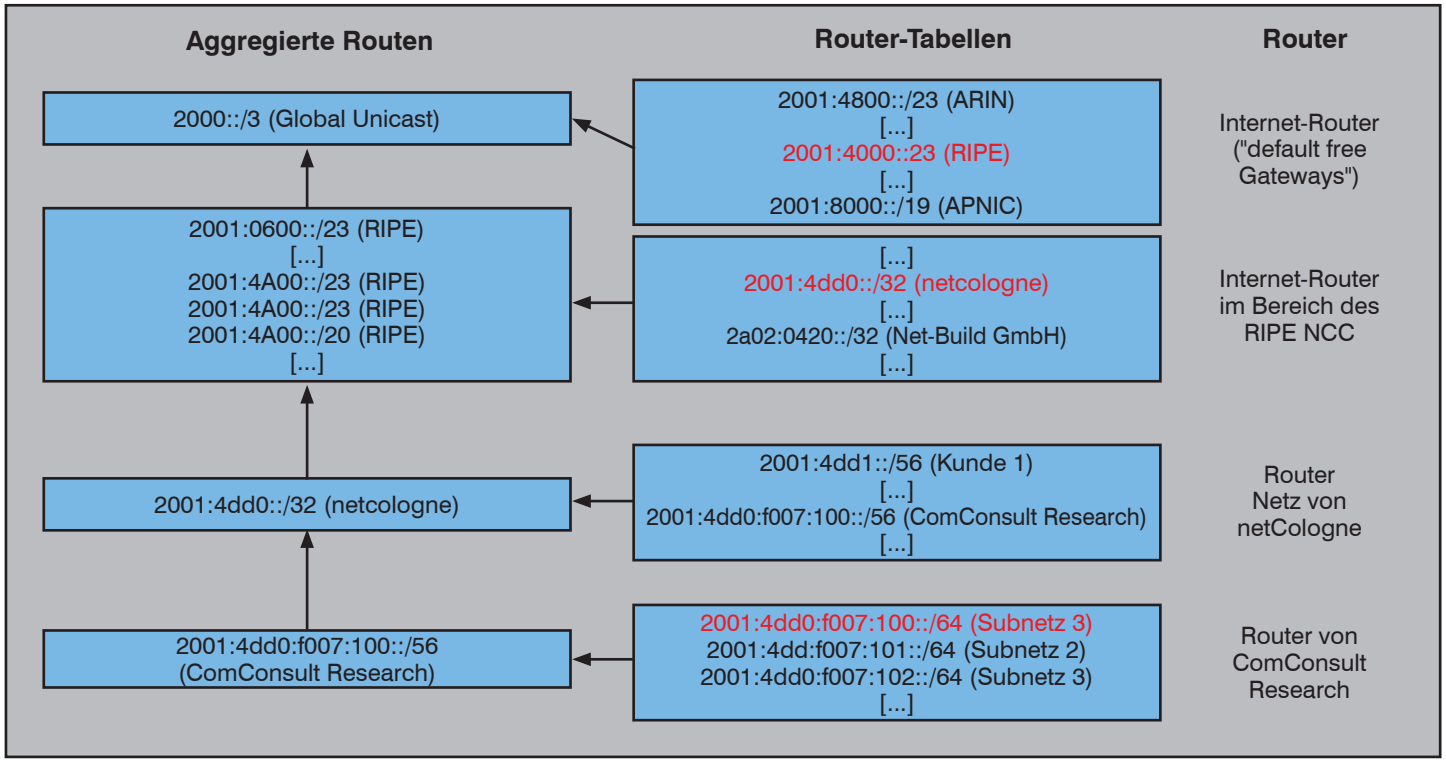


Abbildung 4: Beispiel einer Routen-Aggregierung

IPv6 Adresse: die Qual der Wahl

1. **Lokale Router von ComConsult Research**
   ComConsult Research hat von seinem Provider das Präfix 2001:4dd:f007:100::/56 zugewiesen bekommen.

   Dieser Block wurde in diverse Subnetze aufgeteilt: DMZ, Transfernetz von der Firewall zum ISP Router, Testnetz, Rechnernetz, Servernetz, etc.

   Alle Router von ComConsult Research müssen alle internen Präfixe kennen. Zum Internet jedoch existiert nur eine default Route (::/0).

2. **Router des ISP**
   Der ISP hat vom RIPE NCC den Block 2001:4dd0::/32 zugewiesen bekommen.

   Dieser Block wird nun in unterschiedlich großen Bereichen an die Kunden weitergegeben.

   Die Router des ISP müssen alle diese Kundenpräfixe kennen, jedoch benötigen sie keine Einträge für die Teilnetze, die ihre Kunden daraus gemacht haben.

   Ferner verfügen die (meisten) Router des Providernetzes noch über eine Default Route, die in Richtung eines oder mehrerer Internetknoten wie dem DE-CIX zeigt. Auch diese internen Providerrouter müssen keine Kenntnisse über den Rest der Welt haben.

3. **Grenzrouter / Default Free Gateways / Internet-Knotenpunkte**
   An den Internet-Knoten werden nur die vom RIPE zugewiesenen Blöcke zwischen den Providern ausgetauscht, nicht aber die vergebenen Teilnetze. So weiß Provider A zwar, dass Provider B den Block 2001:4dd0::/32 zugewiesen bekommen hat, nicht aber, welche Unterbereiche davon bereits zugewiesen wurden und welche nicht.

   Ferner müssen Internet-Knoten die Blöcke aller anderen Internetknoten kennen, die sich im Gebiet desselben RIR befinden. Das DE-CIX muss also wissen, welche Netze beispielsweise in den Niederlanden zu finden sind, um Pakete zum dortigen Internet-Knoten routen zu können.

   Für die Verbindung in die Gebiete anderer RIR müssen die Internet-Knoten nur die vom IANA zugewiesenen Blöcke und die Routen dorthin kennen. Die interne Struktur anderer Regionen spiegelt sich in den Routing-Tabellen somit nicht wieder.

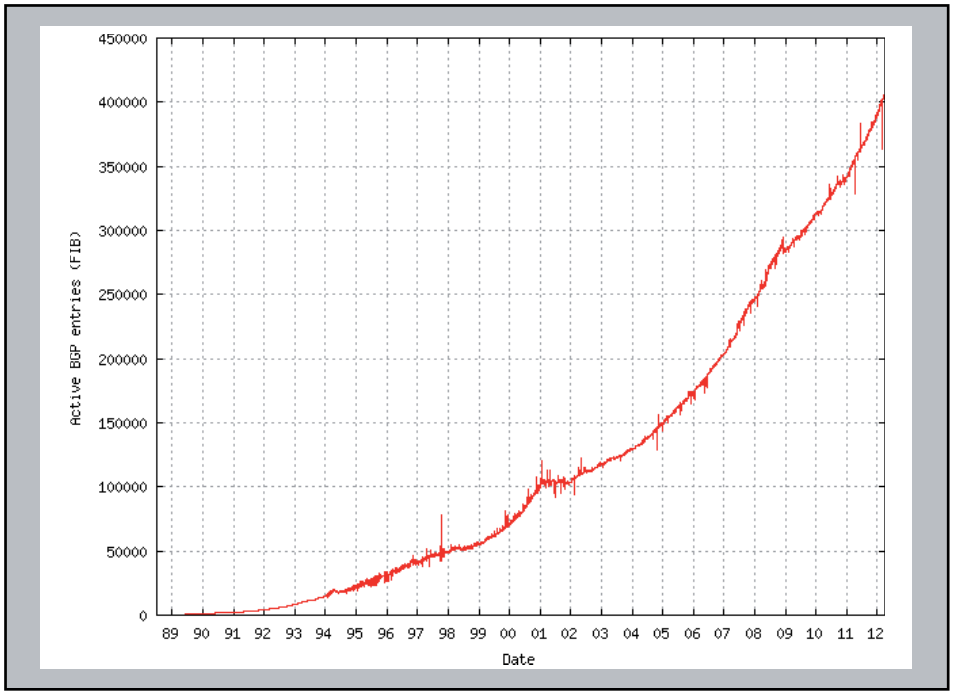


Abbildung 5: Aktive BGP-Einträge (Quelle: CIDR Report)

Die Notwendigkeit dieses Verfahrens wird an Abbildung 5 schnell deutlich. Die Grafik zeigt das Anwachsen der Routingtabellen in Internetroutern von 1989 bis heute für IPv4. Bedenkt man, dass IPv6 praktisch unendlich mal mehr Netze als IPv4 hat, so muss von vornherein ein Verfahren existieren, das diese Routing Tabellen möglichst klein hält. Die theoretische Präfix-Menge von IPv6 macht es schlicht unmöglich, ohne Aggregierung zu arbeiten.

Präfix vom Provider

Das Problem der Aggregierbarkeit zeigt, warum die Verwalter der IPv6 Adressen ein aktives Interesse daran haben, dass End User Präfixe aus den Blöcken der Provider nutzen. End User im Sinne der Registrars sind alle, die keine LIRs sind, also nicht nur Privatanschlüsse, sondern auch Unternehmen und Organisationen aller Art.

Doch die Internetproblematik ist aus Sicht vieler Netzbetreiber eben ein Problem der Internetprovider. Außerdem funktioniert es bei IPv4 ja auch, dann muss es auch mit IPv6 klappen.

Was spricht nun für und was gegen eine Adresse aus dem Bereich des ISP aus Sicht von Unternehmen:

Pro

- **Anwendungen für die keine Proxys / ALGs existieren**
  Es gibt Anwendungen, für die keine ALGs bzw. Proxys existieren. Da mit global routbaren IP-Adressen gearbeitet wird, können sie grundsätzlich betrieben werden. Ob das in Bezug auf die Sicherheit wünschenswert ist, ist eine andere Frage.

- **Künftige Entwicklung von P2P-Anwendungen**
  Siehe oben.

- **Netzdesign**
  Es stehen ausreichend Präfixe für ein skalierbares und zukunftssicheres IP-Design zur Verfügung. Wenn nicht, sollte man seinen Provider um einen größeren Block IPv6-Adressen bitten. Einige Provider glauben zwar noch, dass auch IPv6-Adressen Mangelware sind. Aber sanfter Druck hat sich in der Praxis als hilfreich erwiesen, wenn der Provider knausert.

- **Kleine Routingtabellen**
  Intern und auf den Internet-Zugangsroutern kann mit einer default Route gearbeitet werden. Ein aktiver Austausch von Routen mit dem Provider ist nicht notwendig. Das reduziert die Fehlerwahrscheinlichkeit und den Ausnwand für den Betrieb drastisch.

- **Geringe Kosten**
  Wie bei IPv4 sind Provider-Adressen in den allermeisten Fällen Bestandteil des Internetanschlusses und kosten keinen Aufpreis.

- **Gutes Gewissen**
  Als Betreiber kann man sich ein gutes

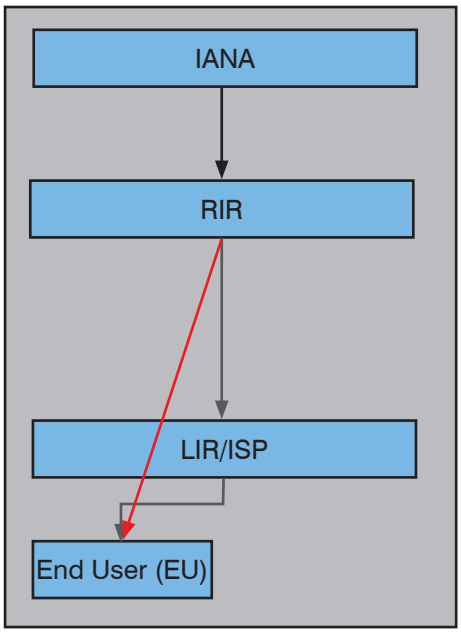


Abbildung 6: Zuweisung von PI Adressen

Gewissen leisten, da man das Internet nicht mit unnötigen Routing-Einträgen belastet.

Contra

- **Providerwechsel**
  Wechselt ein Unternehmen den ISP, so kann es die IP-Adressen nicht weiter verwenden, sondern bekommt einen neuen Präfix-Block aus dem Bereich des neuen Providers. Eine komplette Neunummerierung aller internen Systeme ist die Folge.

- **Firmenfusion**
  Fusionieren zwei Unternehmen, die bei unterschiedlichen ISPs sind, kommt das einem Providerwechsel von zumindest einem der Unternehmen gleich. Eine Neuverteilung der Präfixe auf alle Systeme dieses Unternehmens ist somit unvermeidlich.

- **Dual Homed**
  Ist es notwendig, an auch nur einem Standort an mehr als einen Provider angeschlossen zu sein, so kommen Provider-Adressen nicht mehr in Betracht, da beide ISPs diesen Block in ihrem Netz routen müssen. Auch anderen Providern müssen diese Routen bekannt gegeben werden, damit der optimale Weg berechnet werden kann und es im Fehlerfall eine echte Redundanz gibt.

- **Sicherheit**
  Da die Provider-Präfixes global routebar sind, ist es bei fehlerhafter Firewallkonfiguration grundsätzlich möglich, interne Systeme direkt aus dem Internet zu adressieren und damit direkt anzugreifen.

Auf den ersten Blick überwiegen die Nachteile und ein „gutes Gewissen“ ist wohl kaum ein Argument. Wie also steht es um die Alternative?

Provider unabhängige Adresse

Provider-unabhängige Adressen, kurz PI für „Provider Independent“, kommen aus dem Bereich der RIR Blöcke und sind keinem Provider zugewiesen (vgl. Abbildung 6). Wohl aber sind sie einer Region zugeordnet. Weltweit tätige Unternehmen benötigen somit für jede Internetregion eine eigene PI. Es ist nicht erlaubt, mit einer IPv6-Adresse aus dem Bereich des RIPE NCC in Asien „ins Internet zu gehen“.

Um eine PI zu bekommen, sind einige Formalitäten einzuhalten. Je nach Art des eigenen Unternehmens, insbesondere der Größe, gibt es unterschiedliche Verfahren. Man sollte sich auf jeden Fall beim RIPE NCC erkundigen, welche für einen in Frage kommen und welche Formalitäten beachtet werden müssen. Allen gemeinsam sind jedoch:

- Für die IP-Adressen fallen jährliche Lizenzgebühren an.
- Die IP-Präfixe werden nur verliehen.
- Das RIPE verlangt, dass Anfragen innerhalb von 3 Monaten bearbeitet werden.

Je nach Zuteilungsvariante benötigte man auch noch einen Sponsor in Form seines ISPs, an den dann auch die Lizenzgebühren zu entrichten sind.

Betrachten wir auch für diese Adressen die Vor- und Nachteile:

Pro

- **Dual Homed**
  Das „Totschlagkriterium“: Wer an einem Standort an mehr als einen Provider angeschlossen ist, benötigt zwingend eine PI für alle Systeme, die von extern erreichbar sein müssen.

- **Providerwechsel**
  Ein Providerwechsel macht zunächst keine Probleme, da man die PI definitionsgemäß behalten kann. Jedoch kann es notwendig sein, dass der Sponsor beim RIR von alten auf den neuen ISP geändert wird.

- **Firmenfusion**
  Bei einer Firmenfusion kann das Unternehmen mit den PI-Adressen diese auch für das andere Unternehmen nutzen. Dort allerdings wird trotzdem eine Umnummerierung fällig. Ein echter Vorteil ist das also nur dann, wenn beide Unternehmen PI Adressen haben.

- **Anwendungen für die keine Proxys / ALGs existieren**
  Identisch mit Provider-Adressen.

- **Netzdesign**
  Identisch mit Provider-Adressen.

Contra

- **Sicherheit**
  Da die Provider Präfixes global routebar sind, ist es bei fehlerhafter Firewallkonfiguration grundsätzlich möglich, interne Systeme direkt aus dem Internet zu adressieren und damit direkt anzugreifen.

- **Höhere Kosten**
  Für PI-Adressen fallen Gebühren an.

- **Größere Routing-Tabellen und damit höhere Kosten**
  Nutzt man selbst BGP, im Falle von Dual Homed notwendig, dann wachsen zumindest auf den Internetzugangsroutern die Routing-Tabellen dramatisch an. Je nach Netzdesign sind auch weitere Router davon betroffen. Das führt zu höheren Kosten bei der Beschaffung der Router und vor allem auch im Betrieb dieser Router.

Die Qual der Wahl: ULA, PI, ISP

Fassen wir die möglichen Präfixe noch einmal kurz zusammen, so gibt es 2x2 Varianten:

1. Unique Local Addresses
   a. Global zugewiesen (fc00::/8)
   b. Zufällig erzeugt (fd00::/8)

2. Globale Adressen
   a. Aus dem Pool des ISP
   b. Provider Independent (PI)

Da 1.a zur Zeit nicht existiert, verbleiben somit die anderen drei Möglichkeiten. Die Frage, welche man wählt, ist die vielleicht am kontroversesten diskutierte Frage auf unseren Veranstaltungen. Die zentralen Argumente, die immer wieder angesprochen werden, lassen sich so zusammenfassen:

1. „Eine PI hat den Vorteil, dass ich nie wieder ein Renumbering machen muss."

2. „ULAs bieten mir mehr Sicherheit, da aus dem Internet auf meine Systeme nicht zugegriffen werden kann."

Damit scheint sich die Entscheidung auf zwei der verbliebenen drei Möglichkeiten zu reduzieren. ISP-Adressen scheiden offensichtlich völlig aus. Doch obwohl beide Argumente zunächst plausibel klingen, greifen sie zu kurz.

Betrachten wir zunächst das erste Argument:

PI = nie wieder ein Renumbering?

Das würde voraussetzen, dass man eine einmal zugewiesene PI für die Ewigkeit nutzen kann, was praktisch einem „Besitz" dieser Adresse gleich käme. Und in der Tat, so war es faktisch bei IPv4, da bei deren Vergabe anfänglich kein „Rückholverfahren" vorgesehen war. Daher kommt es auch, dass einzelne Universitäten heute Class A Netze haben oder kleine Unternehmen mit nicht mal 200 Mitarbeitern sich über ein Class B Netz freuen dürfen. Die Konsequenz ist hinreichend bekannt: Adressknappheit.
Diesen Fehler will man bei IPv6 nicht noch mal machen. Darum sehen die Vergaberichtlinien des RIPE NCC für IPv6 Adressen vor, Adressen wieder in den RIPE Pool zurückzuholen. Wörtlich wird von einer gebührenpflichtigen Lizensierung von IPv6 Adressen gesprochen und der Begriff „Besitzt" wird ausdrücklich zurück gewiesen. Im Gegenteil, es wurden eine Reihe von (noch ausschließlich formalen) Richtlinien festgelegt, bei denen die Adressen automatisch in den Pool des RIPE NCC zur erneuten Vergabe zurückwandern. Dazu gehören die Nicht-Entrichtung der jährlichen Lizenzgebühr und die dreimonatige Nicht-Erreichbarkeit des Vertragspartners durch das RIPE NCC.

Nun stellen Sie sich einfach mal vor, sie finden drei Monate lang keinen neuen Administrator und der Vertreter weiß nichts mit „diesen komischen, englischen Nachrichten vom RIPE" anzufangen:

Schwupps ist die IPv6-Adresse weg, wird in der Folge im Internet nicht mehr geroutet und man kann weder das Internet nutzen noch werden die eigenen öffentlichen Server gefunden. Einen Anspruch darauf, die „eigene" Adresse wieder vom RIPE „zurück" zu bekommen, hat man nicht. Bis also alles wieder läuft, kann es lange dauern. Mit einer ISP Adresse wäre das (wahrscheinlich) nicht passiert.

ULAs bieten Sicherheit

Richtig ist: Interne Systeme mit ULAs können nicht direkt aus dem Internet adressiert werden.

Falsch ist: Interne Systeme mit ULAs können aus dem Internet nicht erreicht werden.

Zwei Worte Unterschied – große Wirkung.

Gegen eine ganze Reihe von Angriffen bieten ULAs genau so wenig Schutz wie es heute private Adressen und NAT tun: Viren, Trojaner, Rootkits, DoS-Attaken auf den Internetzugang oder Server/ALGs/Proxys/Firewalls in der DMZ, Phishing, Pharming, etc.

Auf der anderen Seite beeinträchtigen ULAs aber einen ganz anderen Aspekt von Sicherheit: die Zukunftsicherheit des IP-Designs. Sie schließen konsequent die Möglichkeit von P2P-Anwendungen aus. Auf den ersten Blick ein Vorteil, will man diese doch auch gar nicht im Unternehmen haben, da sie nur schwer zu kontrollieren sind. Auf den zweiten Blick jedoch wird schnell klar, dass man sich damit von zukünftigen Entwicklungen ausschließt, die P2P voraussetzen. Aber schon heute gibt es solche Anwendungen vor allem im Kommunikationsumfeld: Die Gesprächs- und Videodaten zwischen IP Telefonen laufen „eigentlich" Ende-zu-Ende, ein Design mit Mediagateways, Session Border Controllern, Gatekeepern und ähnlichem ist zwar möglich und sogar üblich, ist aber immer auch mit Restriktionen bei Skalierbarkeit und Fehlertoleranz verbunden.

IPv6 wird diesen Trend zu P2P-Anwendungen verstärken, da anders als derzeit bei IPv4, die Ende-zu-Ende-Erreichbarkeit wieder üblich werden wird. Eine Möglichkeit, die Entwickler neuer Software sich mit Sicherheit nicht entgehen lassen werden.

Spätestens wenn die erste Anwendung im Unternehmen Einzug hält, für die es keinen Proxy gibt, ist das Ende der ULAs eingeläutet und damit ein Renumbering nicht mehr zu verhindern.

Renumbering: halb so wild?

Die Verteilung neuer IP-Adressen auf alle Systeme ist der Horror eines jeden Netzbetreibers. Darum ist es kein Wunder, dass dieses Argument häufig gegen Provider Adressen angeführt wird. Doch wird dabei übersehen, dass IPv6 zwei entscheidende Änderungen mit sich bringt, die eine Neuverteilung von Adressen vereinfacht und ihr somit einiges an Schrecken nimmt:

1. **IPv6 sieht mehrere IP Adressen pro Interface vor**
   Zwar **erlauben** viele moderne Betriebsysteme mehr als eine IPv4-Adresse pro Interface, aber wie jeder bestätigen kann, der es versucht hat, ist das Ergebnis mehr als unbefriedigend.

   Bei IPv6 ist das nun anders: Endgeräte **müssen** mehr als eine IP-Adresse pro Interface beherrschen, da jedes Interface zumindest eine Locale Adresse und eine routbare Adresse bekommt und beide auch nutzt. Damit ist es aber nur ein kleiner Schritt auch gleich mehrere routbare IP Adressen zuzulassen. Im Falle der Security Extensions für den Host-Anteil ist das sogar notwendig, um beim Adresswechsel zu verhindern, dass bestehende Verbindungen abbrechen.

   Die Folge für ein Renumbering ist, dass es nicht mehr über Nacht und auf allen Geräten gleichzeitig geschehen muss. Vielmehr kann man zunächst die neuen Adressen ausrollen und wenn sie flächendeckend verteilt sind, die alten zurückziehen.

2. **Präfixe werden dynamisch verteilt**
   Die Zuweisung der Präfixe per Router Advertisements oder per DHCP ist die einzig praktikable Möglichkeit bei IPv6 und nur sehr wenige Geräte werden davon ausgenommen sein (Router, Firewalls, DNS-Server etc.).

Bei einem Renumbering kann also von zentraler Stelle aus die Verteilung erfolgen und nur wenige Geräte müssen wirklich angefasst werden.

Also doch ISP-Adressen?

Wie man sieht, gibt es also doch gute Gründe für den flächendeckenden Einsatz von ISP-Adressen: Solange man den Provider nicht wechselt, hat man seine Adressen sicher und ist für zukünftige Entwicklungen gewappnet. Scheinbare Vorteile einer PI wie „Adresse für die Ewigkeit“ existieren nicht oder sind zumindest nicht so sicher, wie es den Anschein hat. Auf der anderen Seite ist zu erwarten, dass die gefürchtete Umnummerierung bei IPv6 viel von ihrem Schrecken verloren hat, auch wenn hier letztendlich der „Beweis“ in der Praxis noch aussteht.

Daraus lässt sich der überraschende Schluss ziehen: Wer nicht zwingend eine PI benötigt, weil er z.B. Dual-Homed ist, ist mit einer Provider Adresse ebenso gut bedient und das bei erheblich geringerem Aufwand der Beschaffung und sichererer Perspektive - solange man den Provider nicht wechselt.

Wie das Beispiel der Adressauswahl zeigt, gilt es bei der Einführung von IPv6 schon früh weitreichende Entscheidungen zu treffen. Themen wie Autokonfiguration und DHCP, Hostanteil der IPv6-Adresse oder Konsequenzen für Sicherheit und Design durch den Wegfall von NAT wurden hier bestenfalls angerissen. Wer sich einen umfassenden Überblick über die Änderungen bei IPv6, deren Konsequenzen, dem aktuellen Stand der Technik und Erfahrungen aus laufenden Projekten verschaffen möchte, sollte das ComConsult IPv6-Forum auf keinen Fall verpassen.

Abkürzungen

ALG	Application Layer Gateway
APNIC	Asia Pacific Network Information Centre
BOOTP	Bootstrap Protocol
DHCP	Dynamic Host Configuration Protokol
DMZ	Demilitarisierte Zone
DNS	Dynamic Name Service
DoS	Denial of Service
IANA	Internet Assigned Numbers Authority
IP	Internet Protokoll
KFZ	Kraftfahrzeug
LIR	Local Internet Registrars
NAT	Network Address Translation
OSPF	Open Shortest Path First
P2P	Peer to Peer
PI	Provider Idependent (Address)
RFC	Request for Comments
RIPE NCC	Réseaux IP Européens Network Coordination Centre
RIR	Regional Internet Registrars
SBC	Session Border Controller
UC	Unified Communication
ULA	Unique Local Address
VoIP	Voice over IP

Literatur

rfc4193.txt - Unique Local IPv6 Unicast Addresses

https://panopticlick.eff.org/browser-uniqueness.pdf - How Unique Is Your Web Browser?

http://www.ripe.net/ripe/docs/ripe-545 - IPv6 Address Allocation and Assignment Policy (RIPE)

http://www.ripe.net/ripe/docs/ripe-452 - Contractual Requirements for Provider Independent Resource Holders in the RIPE NCC Service Region

http://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xml - IPv6 Global Unicast Address Assignments

http://www.cidr-report.org/as2.0/ - CIDR REPORT

Neues Seminar

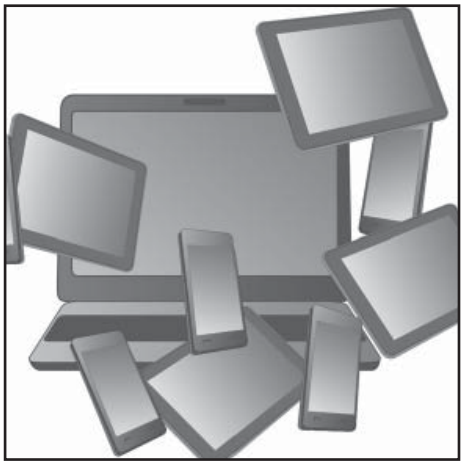
Mobile Device Management - Betrieb von mobilen Endgeräte-Flotten

Die ComConsult Akademie veranstaltet am 10.05.12 erstmalig ihr neues Seminar „Mobile Device Management - Betrieb von mobilen Endgeräte-Flotten“ in Bonn.

Smartphones sind aus dem Arbeitsalltag vieler Mitarbeiter nicht mehr wegzudenken. Durch den Consumer-Markt getrieben, werden auch Tablets für den Unternehmenseinsatz immer interessanter. Aber auch herkömmliche PC-Clients sind durch den Austausch vieler Desktop-Rechner durch Notebooks mobilisiert worden. Mit der Verfügbarkeit von mehr kompatibler Enterprise-Software für Smartphone, Tablet & Co. werden die Grenzen zwischen mobilen Endgeräten und klassischen PC-Clients immer mehr verschwimmen.

Mit der steigenden Mobilität von Mitarbeitern und Endgeräten wird die Unternehmens-IT vor viele Herausforderungen gestellt:

- Service und Support für mobile Endgeräte stellt die bisherigen Betriebskonzepte für Clients in Frage. Ob Vertriebsmitarbeiter oder Teleworker - der Rückruf von Mitarbeitern zum zentralen Service-Standort wegen eines fehlkonfigurierten oder wartungsbedürftigen



Endgeräts ist meist nicht zumutbar.

- Die verkürzten Produktzyklen mobiler Endgeräte und Trends wie Bring Your Own Device (BYOD) sorgen automatisch für eine größere Endgeräte- und Plattformvielfalt. Diese Geräte unter ein einheitliches Management zu stellen ist kompliziert, wenn nicht sogar unmöglich.

- Datensicherheit auf einer großen Vielzahl von Clients sicherzustellen überfordert die Sicherheitskonzepte, die auf ortsfeste Clients angewendet wurden. Die Betriebsverantwortlichen müssen sich die Frage stellen, ob und welche Sicherheitsmaßnahmen auf mobile Endgeräte noch anwendbar sind, und um welche Maßnahmen das Sicherheitskonzept ergänzt werden muss.

Das Gefährdungspotenzial, das von der Mobilisierung der Clients ausgeht, ist erheblich. Ob Datenabfluss oder die Einschleppung von Malware - es ist klar, dass für mobile Endgeräte nicht niedrigere, sondern mindestens gleichwertige Härtungsmaßnahmen getroffen werden müssen. Hierzu ist die Umsetzung von geräteübergreifenden Sicherheitsrichtlinien notwendig. Die Umsetzung erfordert ein leistungsfähiges, zentralisiertes Endgeräte-Management. Diese Plattformen werden auch benötigt, um Service und Support durch leistungsfähige Fernwartungsmechanismen zu unterstützen und Endgerätenutzer wie auch Helpdesk-Mitarbeiter zu entlasten.

Dieses Seminar analysiert den Trend zur Mobilisierung der Unternehmens-IT. Es werden Konzepte und technische Maßnahmen zum Umgang mit diesem Sachverhalt aufgezeigt. Es werden verfügbare technische Lösungen vorgestellt und Strategien für den Betrieb dieser Lösungen erarbeitet.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Mobile Device Management - Betrieb von mobilen Endgeräte-Flotten

Ich buche das Seminar
Mobile Device Management - Betrieb von mobilen Endgeräte-Flotten

☐ **10.05.12 in Bonn**
zum Preis von € 990,-- netto

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

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

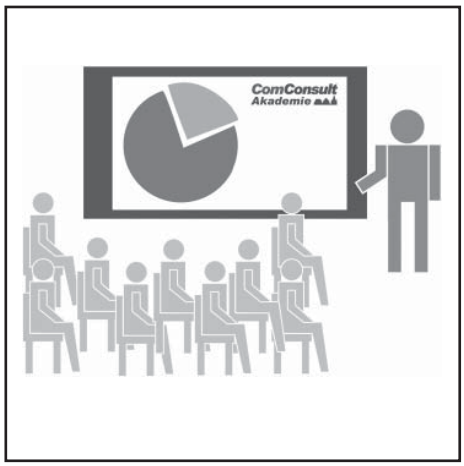
Neues Seminar

Besser und erfolgreich Präsentieren

Die ComConsult Akademie veranstaltet vom 21.05. - 22.05.12 in Aachen und am 18.06.12 in Bonn erstmalig ihr neues Seminar „Besser und erfolgreich Präsentieren".

In diesem Seminar werden auf sehr praktische Weise die neuesten Erkenntnisse zu wirkungsvollen Präsentationen aus der Geschäftspraxis sowie aus der Forschung vorgestellt und gemeinsam erarbeitet. Basierend auf Lars Sudmanns langjähriger Erfahrung als Führungskraft, Trainer sowie als 'Champion Speaker' liefert Ihnen dieses Seminar ein Feuerwerk von Tipps und Strategien, mit denen Sie Ihre Präsentationen eindrucksvoll und inspirierend gestalten können. Lernen Sie von einem Europameister der Rhetorik, der nationale und Internationale Erfolge gefeiert und weitreichende Erfahrungen in der Unternehmenspraxis gesammelt und der mit vielen interessanten Strategien schon Tausende von Fach- und Führungskräften in Europa begeistert hat.

Methodik
Das Seminar nutzt moderne Gestaltungen der Trainingspraxis wie Accelerated Learning, Erkenntnisse der Gehirnforschung, Multimediatechniken und vieles mehr für ein lebhaftes Training. Die Teilnehmerzahl ist auf 10 Personen begrenzt für einen maximalen Lernerfolg. Jeder Teilnehmer wird mehrfach präsentieren und den Inhalt direkt in die Praxis umsetzen können. Detailliertes und persönliches Feedback - auch per Videoanalyse- sowie Checklisten runden das Training ab.



Das Konzept
2 Tage Theorie- und Praxistraining + Übungsphase im Berufsalltag + 1 Tag Praxischeck

2 Tage Theorie- und Praxistraining
Die ersten zwei Seminartage gehen mit einer Vielzahl von Übungs- und Theorieelementen auf Ihre persönlichen Präsentationen ein. Wir behandeln Beispiele aus Ihrer Geschäftspraxis (natürlich vertraulich und nach Ihrem Ermessen) und keine theoretischen Fallstudien.

1 Tag Praxischeck
Nach dem Besuch des ersten Seminarteils haben sie 4 Wochen die Gelegenheit, das Gelernte in Ihrem beruflichen Alltag in die Praxis umzusetzen. Danach besuchen Sie den zweiten Teil des Seminars. Sie halten vor der Gruppe Ihre eigene Präsentation. Durch das Feedback des Trainers und weiter aufbauende Übungen, Tipps und Tricks haben Sie am Ende dieses Tages Ihren Lernerfolg weiter optimiert.

In diesem Seminar lernen Sie
- Welche Präsentationsform passt zu welchem Anlass?
- Wie lasse ich beim Publikum einen professionellen und bleibenden Eindruck? Wie wirke ich auf andere?
- Wie vermeide ich lange Vorbereitungen mit MS Power Point™?
- Wie erziele ich einen guten ersten Eindruck und wie gehe ich mit dem Lampenfieber in den ersten Minuten um?
- Wie stelle ich komplexe Themen (beispielsweise Daten und Modelle) optimal dar, ohne jedoch zu stark zu vereinfachen?
- Wie baue ich eine wirkungsvollen roten Faden und eine Story auf?
- Wie schaffe ich es, dass mein Publikum auch noch 45 Minuten noch frisch und gespannt ist?
- Wie strukturiere ich meine Präsentation für maximalen Erfolg?
- Wie binde ich verschiedene Teilnehmergruppen optimal ein (Entscheider, Experten, Neulinge,,..)
- Wie gestalte ich meine Folien und visuellen Hilfsmittel optimal und ohne zu viel Aufwand?
- Was ist die optimale Anzahl von Folien? Gibt es überhaupt eine optimale Anzahl?
- Wie gehe ich auf schwierige Fragen und Teilnehmer ein?
- Bei Bedarf und Interesse - wie präsentiere ich ‚virtuell' in Telefon- und Videokonferenzen?

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Besser und erfolgreich Präsentieren

Ich buche das Seminar
Besser und erfolgreich Präsentieren

☐ **21.05. - 22.05.12 in Aachen und 18.06.12 in Bonn**

zum Preis von € 1.990,-- netto

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

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

Standpunkt Sicherheit

Wenn die Informationssicherheit überreagiert

Der Standpunkt Sicherheit 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.

Es kommt durchaus vor, dass durch Veränderungen in der IT-Konfiguration bestehende IT-Sicherheitsrichtlinien verletzt werden. Bei genauerem Hinschauen zeigt sich dann nicht selten, dass eine Richtlinie zu scharf formuliert und letztendlich einfach ignoriert worden ist.

Beispiel: Eine Netzzugangskontrolle soll in einem Unternehmen eingeführt werden, da im Rahmen eines Audits erhebliche Risiken durch den ungesicherten Netzzugang festgestellt wurden. Gleichzeitig wird die Anforderung gestellt, dass Geräte, die sich nicht erfolgreich authentisieren können (z.B. weil ihr Zertifikat abgelaufen ist oder ganz einfach, weil der PC noch einen PXE-Boot-Vorgang bearbeiten und zum Laden des Betriebssystems erst mit der Infrastruktur kommunizieren muss), einen eingeschränkten Netzzugang zu Wartungszwecken bzw. zur Softwareverteilung erhalten. Ähnliches gilt für Geräte, die zwar an das Netz gelassen werden müssen, sich aber nur mit einem Authentisierungsmittel geringer Güte ausweisen können. Das entsprechende Konzept hat hierzu eine Authentisierung am Netzwerkport in Verbindung mit einer dynamischen durch RADIUS gesteuerten logischen Trennung der Gruppen per VLAN und VRF vorgesehen. Die Übergänge zwischen Gruppen würden durch eine zentrale Firewall abgesichert. Das Konzept wird dem IT-Sicherheitsbeauftragten (ITSB) vorgelegt, der es mit dem Hinweis kategorisch ablehnt, dass gemäß einer Sicherheitsrichtlinie VLANs zur Trennung von Netzen unterschiedlichen Sicherheitsniveaus nicht gestattet seien.

Ähnliche Situationen sind aus anderen Fällen bekannt, wo es z.B. um die Trennung von Gruppen in einem WLAN oder um die Zonierung und Virtualisierung im Rechenzentrum ging.

Welche technische Alternativen hätten in dem genannten Beispiel bestanden? Wenn keine dynamisch aktivierte ACLs auf den Access Switches zum Einsatz kommen können (was meist ein geringeres Sicherheitsniveau darstellt), bleiben nur der Aufbau einer nicht betreibbaren Lösung, der Verzicht auf den Einsatz einer Netzzugangskontrolle oder man macht es einfach trotzdem wie geplant. Die Folge könnte daher sein, dass Vorgaben des ITSB bei Infrastrukturprojekten und anderen Changes künftig immer öfter einfach ignoriert werden.

Das beschriebene Beispiel illustriert zwei Problembereiche:

Erstens mag die zugrundeliegende Sicherheitsrichtlinie zwar schön konkret sein, sie ist jedoch zu streng und geht an den Realitäten in der modernen IT (hier der Virtualisierung) vorbei. Die Richtlinie hätte besser Kriterien liefern müssen, wann unterschiedliche Systeme physikalisch (oder mit einem vergleichbar starken Mittel) zu trennen sind und wann eine logische Trennung erlaubt ist. Es werden leider zu oft in Sicherheitsrichtlinien Maximalforderungen gestellt. Dies passiert nicht zuletzt deshalb, weil sich der ITSB auf der sicheren Seite wähnen möchte („lieber mehr Sicherheit als zuwenig“) und selber die eigenen Richtlinien nicht umsetzen muss. Außerdem hinken Sicherheitsrichtlinien oft der Zeit hinterher und werden von Innovationen in der IT überholt. Es ist eine Kunst, gute und nachhaltig umsetzbare Sicherheitsrichtlinien zu entwickeln und dabei stets den aktuellen Stand der Technik in der IT reflektieren.

Zweitens hat in dem Beispiel der ITSB eine zwar standfeste aber vielleicht zu kompromisslose Haltung eingenommen. Wahrscheinlich wäre es besser gewesen, als Vermittler zwischen dem Wunschzustand einer Richtlinie und dem Alltag in der IT aufzutreten. Das Ergebnis hätte ein ausgehandelter Kompromiss sein können, der eine gute Balance zwischen Machbarkeit, Wirtschaftlichkeit und Restrisiko dargestellt hätte. Dass eine solche Kompromissfindung aufwendig sein kann und ggf. nicht das gewünschte Sicherheitsniveau darstellt, ist nicht schön, ist aber besser als nichts und insbesondere besser als eine Richtline zu ignorieren. Wenn sich der ITSB als aktiver Lösungsarchitekt sieht, dessen Sicherheitsgebäude kein Luftschloss werden, sondern akzeptiert und so einen nachhaltigen Bestand haben soll, kommt er um diese Rolle des Vermittlers auch nicht herum. Letztendlich ist die im Beispiel beschriebene Kompromisslosigkeit auch ein Zeichen eines nicht richtig gelebten Risikomanagements und damit seinerseits sogar ein Sicherheitsrisiko.

Wichtig ist also, dass der ITSB nicht nur Richtlinienkompetenz hat, sondern sich auch aktiv an der Umsetzung seines Richtlinienapparats beteiligt und vielleicht sogar hieran (zu einem gewissen Anteil) sein Erfolg gemessen wird.

Zweitthema

Die Post-PC-Ära und ihre Auswirkungen

Fortsetzung von Seite 1

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

Dr.-Ing. Behrooz Moayeri hat viele Großprojekte mit dem Schwerpunkt standortübergreifende Kommunikation geleitet. Er gehört der Geschäftsleitung der ComConsult Beratung und Planung GmbH an und betätigt sich als Berater, Autor und Seminarleiter.

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

Der ökonomische Mechanismus der Consumerization basiert darauf, dass ein Massenmarkt, nämlich der Endverbrauchermarkt, den kleineren Markt, den Markt der Unternehmens-IT, dominiert, sobald er zum Massenmarkt geworden ist. Mit Hardware und Software, die in Stückzahlen von hunderten Millionen vermarktet wird, kann keine vergleichbare, für die Abnahme in viel kleineren Mengen konzipierte Technik auf Dauer konkurrieren. So wurden Terminals, bis in die 1980er Jahre die Endgeräte der Unternehmens-IT, von den PCs verdrängt.

Aber nach 30 Jahren geht nun die PC-Ära zu Ende. Was bedeutet das? Das bedeutet vor allem, dass die Dominanz des Geräts Personal Computer in der Informationstechnik endet. Die in der Abbildung 1 wiedergegebene Statistik der International Telecommunications Union (ITU) macht dies deutlich.

Was sagt uns die Statistik? Vor allem dies:

- Während es weltweit ungefähr eine Milliarde PC-Benutzer gibt, hat sich in den letzten fünf Jahren die Zahl der Internet-Benutzer auf über zwei Milliarden verdoppelt.
- Während die Zahl der Festnetztelefonanschlüsse seit Jahren auf dem Niveau von ca. einer Milliarde stagniert und sogar leicht rückläufig ist, hat sich binnen fünf Jahren die Zahl der Mobilfunkteilnehmer auf fast 6 Milliarden mehr als verdoppelt.
- In nur fünf Jahren stieg die Zahl der für Datenübertragung genutzten Mobilfunksubskriptionen (ITU-Bezeichnung: „Mobile Broadband“) von einem nicht

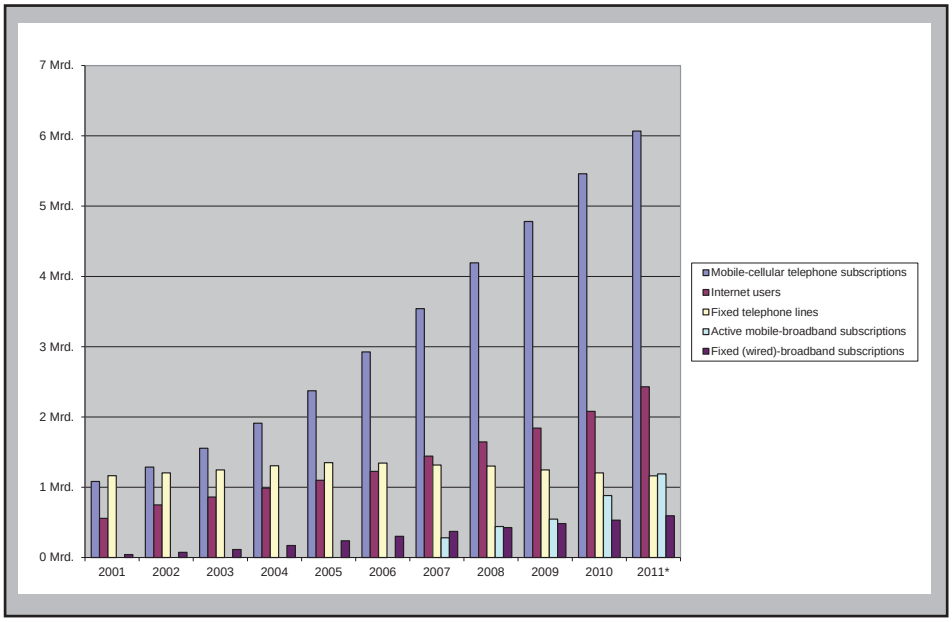


Abbildung 1: ITU-Statistik (Quelle: Thomas M. Chen, IEEE Network, Nov./Dez. 2011)

messbaren kleinen Wert auf die Zahl der Telefonfestnetzanschlüsse, nämlich eine Milliarde.

- Folglich wird das Wachstum der Zahl der Internet-Nutzer im Prinzip durch die mobilen Geräte vorangetrieben. Der PC-Bereich stagniert.

Natürlich verschwindet der PC nicht aus unserem Leben. Es gibt hunderte Millionen Menschen wie die Autoren dieses Beitrags, für die der PC nach wie vor das wichtigste Tor zur IT und zum Internet bleibt. Aber wir haben es mit einem relativen Bedeutungsverlust des PCs zu tun. Die IT- und Internet-Nutzung verlagert sich immer stärker weg vom PC zu neuen Gerätetypen, vor allem Smartphones und Tablets. Die Post-PC-Ära hat schon begonnen, zumindest im Verbrauchermarkt.

Die Folgen für die Kommunikation von Menschen in Unternehmen

Dies kann nicht ohne Auswirkung auf die IT in Unternehmen bleiben. Genauso wie der PC vom Verbrauchermarkt aus Einzug in die Unternehmens-IT fand, finden neue Gerätetypen wie Tablets den Weg vom Verbraucher- in den Unternehmensmarkt. Der Anwender – aus dem Konsumentenmarkt längst schnelle Innovationzyklen und intuitive Bedienkonzepte gewohnt – schleppt „seine" Endgeräte und Applikationen in das Unternehmen ein und fordert ein vergleichbares Nutzungserlebnis – ein Alptraum für IT-Verantwortliche und Sicherheitsbeauftragte. Doch bei allen Schattenseiten haben Entwicklungen wie Bring-Your-Own-Device (BYOD) auch ihre guten Seiten – die IT verjüngt sich und wird agiler, nutzergerechter und damit effizienter.

Ein gutes Beispiel für die positiven Seiten der Consumerization ist die Nutzung von sozialen Medien und Web-2.0-Technologie im Unternehmen. Ob der CIO bloggt, F&E die häufigsten Kundenbeschwerden per Social-Media-Schnittstelle analysieren lässt, Mitarbeiter intern ihr Wissen per Foren aggregieren und teilen, oder zur Aufnahme und Dokumentation von Geschäftsprozessen Wikis als Alternative zum QM-Handbuch genutzt werden – das Potenzial der nutzerzentrierten Web-2.0-Lösungen ist groß. Hierbei spielen, neben dem Mitwirkungscharakter, auch die intuitive Bedienbarkeit und der hohe Wiedererkennungswert durch den privaten Erfahrungshorizont eine große Rolle. Genau das sind die Faktoren, die auch mobile Endgeräte für den Unternehmenseinsatz interessant machen. Und das geht weit über den typischen Vorstandwunsch nach Push-Mail auf dem iPhone hinaus.

Durch ihre Portabilität, ihre Multifunktionalität und die flexible Erweiterbarkeit anhand von App-basierter Technologie erschließen sich mobile Endgeräte viele neue Anwendungsbereiche. Die Einsatzmöglichkeiten reichen von Präsentationszwecken im Vertrieb, über IT-gestützte Arbeiten in der Lagerhaltung bis hin zum Einsatz als universelle, persönliche Kommunikationszentrale. Dabei werden zusehends Aufgabenbereiche „klassischer" PCs erobert. Noch ist es zu früh um abzusehen, ob der PC, wie wir ihn heute kennen, irgendwann ganz ausgedient haben wird. Noch schränken dafür die neuen Gerätetypen in puncto Funktionsumfang und Nutzerschnittstelle ihre Benutzer zu sehr ein. Aber wer weiß, ob es bei diesen Defiziten bleibt oder die neuen Geräte bald keinen Wunsch des klassischen PC-Benutzers mehr offen lassen.

Mit dem PC verlieren auch Konzepte und Begriffe an Bedeutung, die eng mit dem PC verbunden sind. Zu diesen Begriffen gehört Unified Communications, wie sie zumindest von einem Großteil des Marktes verstanden wurde. Mit Unified Communications haben viele die Bündelung und Verknüpfung mehrerer Kommunikationskanäle auf einer PC-Plattform bezeichnet. Dieses Konzept war für die PC-Ära schlüssig, ist aber nunmehr überholt. Wenn Unified Communications tatsächlich die Produktivität steigern und die Arbeitsabläufe beschleunigen soll, muss sie vor allem die Benutzer in den Mittelpunkt stellen - Benutzer, die bereits heute zumeist über andere Geräte als PCs vernetzt sind und kommunizieren.

Die Folgen für die IT-Sicherheit

Die neuen Geräte sind mobil. Damit stellt sich die Frage, wie diese Geräte und insbesondere die auf ihnen gespeicherten Daten geschützt werden können. Was passiert bei einem Diebstahl, der bei mobilen Geräten wahrscheinlicher ist als bei stationären? Wie ist zu verhindern, dass in solchen Fällen vertrauliche oder gar geheime Daten des Unternehmens in falsche Hände geraten, gar Diebstähle genau mit diesem Ziel durchgeführt werden? Konzepte für Data Loss Prevention, die seit Jahren schon für diverse Endgeräte diskutiert werden, bekommen in der Post-PC-Ära noch größere Dringlichkeit. Ohne ein solches Konzept ist die Nutzung der neuen Geräte in der Unternehmens-IT grob fahrlässig.

Ein konsequenter Ansatz wäre Server-Based Computing (SBC). Mit SBC verlassen die Daten nicht den geschützten RZ-Bereich. Die Verarbeitung und Speicherung der Daten erfolgt so weit wie möglich im Data Center. Die mobilen Geräte übernehmen lediglich die Präsentation der Daten. Damit wird das Risiko der Datenkompromittierung zwar nicht vollständig beseitigt, aber minimiert. Nur die auf dem Endgerät zwecks Präsentation zwischengespeicherten Daten würden unter Umständen preisgegeben, wenn das Endgerät verloren ginge. Abbildung 2 illustriert dies am Beispiel Citrix.

SBC ist hier als allgemeiner Ansatz zu verstehen und nicht im engeren Sinn, der von manchen Herstellern für eine bestimmte SBC-Variante, zum Beispiel für den Ansatz mit Terminalservern, verwendet wird. Auch die Präsentation der Daten

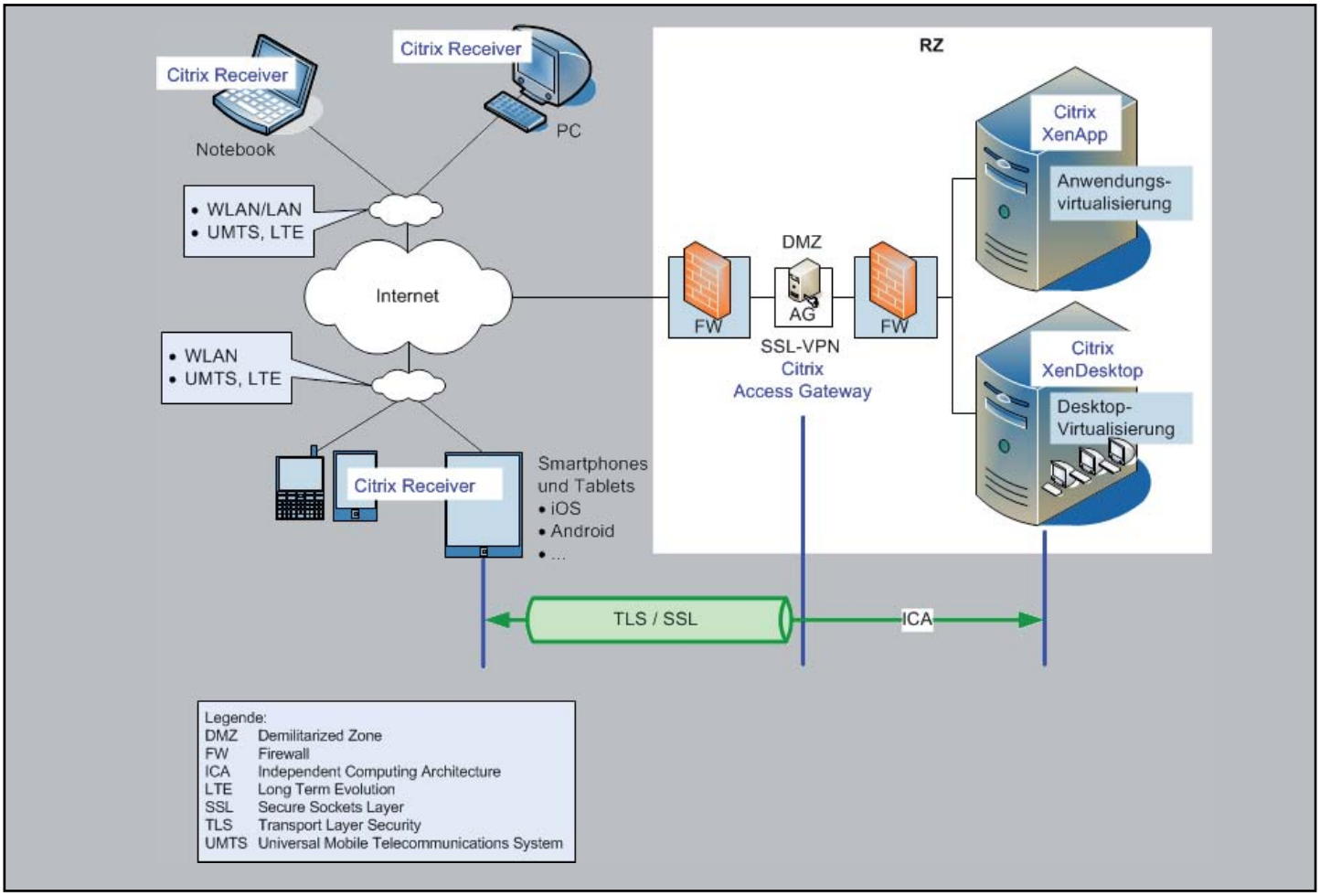


Abbildung 2: SBC am Beispiel Citrix

über eine Webschnittstelle ist im weiteren Sinne als eine SBC-Variante zu verstehen. Selbstverständlich darf die Präsentation der Daten nur nach erfolgreicher Authentisierung des Benutzers erfolgen. Ob sowohl das Endgerät als auch der Benutzer oder nur der Benutzer authentisiert wird, hängt vom Schutzbedarf, von der Wahrscheinlichkeit verschiedener Verlustszenarien, vom Gerätetyp, von der Anwendung und vielen weiteren Faktoren ab.

HTML5 ist ein heißer Kandidat, um Präsentation und Bearbeitung via Webschnittstelle zu realisieren. Während die Einbindung von Mediendaten (Video- und Audio-Tag) im Fokus liegt – was neue Gestaltungsspielräume zur Realisierung von Kommunikations- und Kollaborationslösungen eröffnet – wird Sandboxing bisher nur unbefriedigend realisiert. Ein Sandbox-Tag wird die Kapselung von Daten und Code ermöglichen und dient in erster Linie dazu, potentiell gefährliche Inhalte „einzusperren". Bordeigene Mittel zur Verschlüsselung und Kapselung von Daten nicht nur auf dem Transportweg, sondern auch gegen Client-seitige Attacken, sind momentan nicht in ausgereifter Form verfügbar. Mögliche Ansätze sind Java-basierende Verschlüsselungsbibliotheken. Bis zu einer universellen, Plattform- und Browserunabhängigen Lösung zum Schutz von Applikationsdaten ist es aber noch ein längerer Weg. Eine solide Lösung dieser Problematik ist aber Grundvoraussetzung, um sichere, Web-basierende Applikationsbereitstellung nicht nur in unsicheren Netzen, sondern auch in unreglementierten Client-Szenarien à la BYOD zu ermöglichen.

Eine konsequente zentrale Speicherung und Verarbeitung von Daten im Sinne von SBC hat allerdings Grenzen, da eine performante Online-Anbindung erforderlich wäre. In der Praxis ist ein Caching von Daten auf dem Endgerät ebenso erforderlich, wie die temporäre Bereitstellung entsprechender Anwendungen, was letztendlich auf Application Streaming in einem besonders geschützten Container (d.h. in einer Sandbox) auf dem Endgerät hinausläuft. Interessanterweise sind SBC und Application Streaming genau die Strategien, die in modernen Lösungen für BYOD im Vordergrund stehen.

Wenn die größtmögliche Vermeidung der Speicherung von Daten auf mobilen Geräten, also der zahlenmäßig wichtigsten Gruppe von Geräten, als Mittel der Wahl zur Absicherung der Daten gilt, stellt sich die Frage, ob für solche Geräte die Unterscheidung zwischen vertrauenswürdigen und nichtvertrauenswürdigen Netzen überhaupt sinnvoll ist. Für solche Geräte sind konsequenterweise alle Netze als nichtvertrauenswürdig einzustufen. Diese Geräte, die meistens über das überall verfügbare Internet kommunizieren, sind so zu konzipieren, dass immer von der Kommunikation über ein unsicheres Medium auszugehen ist. Der Aufbau einer besonderen Netzinfrastruktur für mobile Geräte ist in einigen Fällen nicht mehr sinnvoll:

- Wenn die mobilen Geräte ohnehin meistens über ein öffentliches, von einem Service Provider betriebenes Netz kommunizieren, ist nur dafür zu sorgen, dass ein solches Netz auch in den Räumlichkeiten des Unternehmens selbst verfügbar ist. Service Provider können mit besonderen Maßnahmen wie zum Beispiel Femtozellen, Hot Spots, Basisstationen mit begrenzter

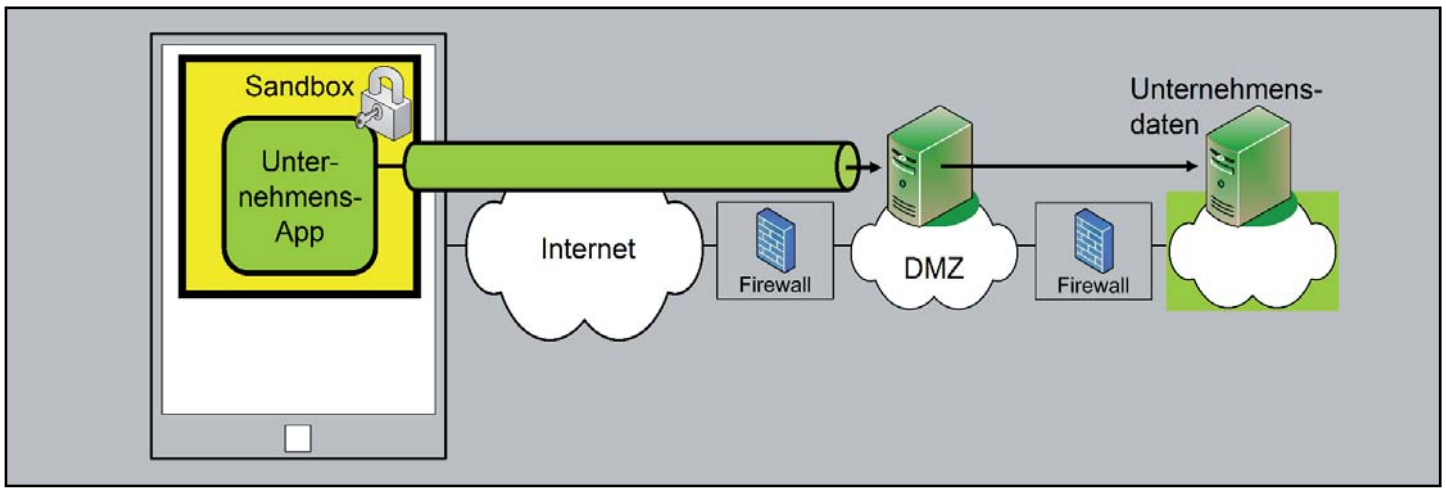


Abbildung 3: Einsatz von Sandboxing

Reichweite oder mit einfachen Signalverstärkern dafür sorgen.

- Wenn für Gäste ohnehin flächendeckend ein Internet-Zugang zu ermöglichen ist, können die eigenen mobilen Geräte des Unternehmens dieselbe Infrastruktur nutzen wie die Gäste.

Ein Teil der Netzinfrastruktur in den Räumlichkeiten des Unternehmens wird somit zur Verlängerung des Internet. Technisch gesehen ist es unerheblich, wer dieses Internet-Zugangsnetz betreibt, ein öffentlicher Service Provider oder das Unternehmen selbst. Diese Herangehensweise hat allerdings Konsequenzen. Sind – zumindest – Teile des LAN eine unsichere Umgebung im Sinne des Internet, so müssen die hierüber angebundenen Endgeräte entsprechend gehärtet sein. Zudem müssen die Anbindung an kritische Ressourcen und der Datentransport gesichert werden. Sowohl für Medienströme als für auch Daten und Dokumente ist eine Ende-zu-Ende-Verschlüsselung damit zwingend. Nur so kann man die Sicherheitsproblematik umgehen, dass unsichere Endgeräte via VPN auf schutzbedürftige Netzbereiche zugreifen können und müssen. Diese Problematik erstreckt sich keinesfalls nur auf Endgeräte der Bauart Smartphone und Tablet. Auch potentiell kritische, lokale Einrichtungen, wie z.B. Drucker, müssen sicher angesteuert werden können. Hierzu zählt selbstverständlich die gesicherte Übertragung von Druckaufträgen, aber auch die Anbindung an zentrale Instanzen wie Messagingserver, um scheinbar triviale Funktionen wie Scan-to-Mail realisieren zu können. Plötzlich handelt es sich bei diesen Geräten um angreifbare Fat-Clients in einer unsicheren Netzumgebung. Andere ortsgebundene Endgeräte, wie z.B. Android-basierende Arbeitsplatztelefone mit Thin-Client-Funktionalität unterliegen derselben Problematik. Es muss also ein ganzheitliches Sicherheitskonzept her, das sowohl Transport- als auch Endgeräte-seitig die Sicherheit der verarbeiteten Informationen gewährleistet, wenn der Bogen von der Post-PC- zur Internet-Ära geschlagen werden soll

Post-PC-Ära = Internet-Ära

Die Internet-Kommunikation gewinnt ohnehin an Bedeutung. Wenn es wahr ist, dass Public Clouds zumindest für einige Unternehmen an Bedeutung gewinnen, dann ist auch wahr, dass das Internet für diese Unternehmen ebenso an Bedeutung gewinnt, denn der Zugriff auf die Public Cloud erfolgt in der Regel über das Internet.

Damit muss sich automatisch auch die Informationssicherheit wieder stärker ihres Namens besinnen: Die reine Kapselung der Daten an physischen Orten (z.B. im heimatlichen RZ) reicht nicht mehr aus. Sicherheitsmechanismen müssen stärker an den Daten selbst verankert werden und unabhängig vom Ort wirken. Dies bedeutet den Einsatz von kryptographischen Techniken, die über Verschlüsselung und Integritätsschutz deutlich hinausgehen. Hier sind Mittel gefordert, die wir eher aus der Welt des Digital Rights Management (DRM) kennen und die beispielsweise dazu dienen können, einen Sicherheitskokon um Daten zu schaffen, innerhalb dessen (ggf. mit zeitlicher Befristung) sicher auf Daten zugegriffen werden kann. Hiermit können dann auch revisionssichere Historien der Datenveränderung zusammen mit den Daten gespeichert werden und das Configuration Management der IT ist endlich von der „Technik“ bei der „Information“ selbst angelangt.

In dem Maße, in dem der Internet-Zugang für Unternehmen geschäftskritisch wird, verlagert sich die Bedeutung von privaten Netzen in Richtung Internet. Viele Unternehmen haben in den letzten Jahren ohnehin festgestellt, dass der hohe Preis, den sie zum Beispiel für private Wide Area Networks zahlen, keinesfalls durch ein Mehr an Zuverlässigkeit im Vergleich zum Internet gerechtfertigt ist. Häufig ist das Umgekehrte der Fall. Viele Netzverantwortliche können sich aus der Erfahrung der letzten Jahre an mehr Probleme mit dem privaten WAN erinnern als mit dem Internet-Zugang.

Das Internet ist für die meisten Unternehmen schon längst eine kritische Infrastruktur. Wenn man von einem „Internet-Unternehmen“ spricht, denken wir aus Gewohnheit häufig an solche Firmen wie Amazon. Diese Assoziation ist irreführend. Auch ein typischer Automobilhersteller, also ein produzierendes Unternehmen, ist schon längst zu einem hohen Maße vom Internet abhängig. Zwar kann man ohne das Internet weiter produzieren, aber keine oder kaum Autos mehr verkaufen. Der Vertrieb vieler produzierender Unternehmen funktioniert heute hautsächlich über das Internet. Je länger der Ausfall der Internet-Kommunikation dauert, desto mehr Umsatz verliert das Unternehmen.

Somit hat das Internet für jedes Unternehmen einen ähnlichen Stellenwert wie das Energieversorgungsnetz, das Wasserleitungsnetz oder das Verkehrsnetz. Es gab Zeiten, in denen auch die Energieversorgung, die Wasserversorgung und das öffentliche Verkehrswesen keine so zentrale Bedeutung für die ganze Gesellschaft hatten wie heute. Damals haben viele Unternehmen für ihre eigene Energieversorgung, ihre eigene Wasserversorgung und ihr eigenes Straßen- und Schienennetz gesorgt. Die wenigsten Unternehmen müssen das heute tun, dank der kritischen Infrastruktur, die unter dem Schutz der Staaten steht.

Die Post-PC-Ära und ihre Auswirkungen

Viele unserer Gewohnheiten, Denkweisen und Praktiken sind Relikte aus Zeiten, in denen es kein Internet mit seiner heutigen Bedeutung für die heutige Gesellschaft gab. Wenn in Zukunft ohne Internet das öffentliche Leben zusammenbricht, dann muss vor allem der Staat dafür sorgen, dass dies nicht eintritt. Nicht zufällig haben zum Beispiel in Deutschland die entsprechenden Stabsstellen der öffentlichen Verwaltung ihre Arbeit schon aufgenommen. Dies bedeutet nicht, dass alle Aufgaben in diesem Zusammenhang vom Staat selbst übernommen werden. Das ist bei anderen kritischen Infrastrukturen auch nicht der Fall. Aber der Staat schafft den Rahmen, regelt die Zuständigkeiten, verordnet die notwendigen Maßnahmen.

Im Rahmen dieser gemeinsamen Anstrengung verschiedener gesellschaftlichen Kräfte - vor allem Staat und Unternehmen - entfällt häufig die Notwendigkeit besonderer vertraglichen Regelungen zwischen einzelnen Instanzen. Service Level Agreements mit Vertragsstrafen bei Nichteinhaltung einer Mindestverfügbarkeit zwischen einem Energieversorgungsunternehmen (EVU) und dessen Kunden sind nicht die Regel. Das EVU muss ohnehin aufgrund seiner gesetzlich geregelten Verpflichtungen das Energieversorgungsnetz in Stand halten. Zu den so zu schützenden Infrastrukturen zählt eigentlich heute schon das Internet. Der lange Zeit geltend gemachte Vorteil eines privaten WAN, für dieses stehe ein bestimmter Vertragspartner gemäß SLA gerade, gilt dann nicht mehr. Erstens haben diese SLAs in den letzten Jahren meistens auch nicht für mehr Verfügbarkeit als die des Internet gesorgt. Zweitens ist das im Vergleich zum privaten WAN vermeintlich nicht so wichtige Internet heute für eine zunehmende Anzahl von Unternehmen mindestens genauso kritisch. Drittens kommt man über das private WAN allein meistens nicht zur Public Cloud; dafür braucht man das Internet.

Haben private Netze ausgedient?

Heißt das, dass das Zeitalter privater Netze vorbei ist? Nein, genauso wenig wie private Strom-, Wasser- und Verkehrsnetze haben private Kommunikationsnetze ausgedient.

Manches Produktionsunternehmen leistet sich das eigene Kraftwerk, um nicht vollständig vom öffentlichen Netz abhängig zu sein oder weil das öffentliche Netz die vom Unternehmen benötigte Leistung nicht so wirtschaftlich oder zuverlässig bereitstellen kann wie das Unternehmen selbst. Viele landwirtschaftliche Betriebe in trockenen Ländern müssen für ihre eigene Wasserversorgung aufkommen. Auch für private Kommunikationsnetze bleiben solche Fälle der Daseinsberechtigung. Beispiele:

- Ein produzierendes Unternehmen kann das Netz, das von seiner Fertigung für die Kommunikation zwischen den verschiedenen Bereichen einer hoch automatisierten Produktion genutzt wird, nicht als Verlängerung des Internet betreiben. Wenn es erforderlich ist, muss es auch ein privates WAN geben, das verschiedene Werke miteinander verbindet und weitgehend von anderen Netzen abgeschottet ist.

- Alle Applikationen und Daten, die aus verschiedenen Gründen nicht in die Public Cloud oder eine anders bezeichnete fremdbetriebene Infrastruktur verlagert werden, brauchen ein eigenes RZ. Entsprechend dem Schutzbedarf dieser Applikationen und Daten muss das RZ-Netz geschützt werden. Dieses Netz ist angesichts der besonderen RZ-Anforderungen auch anders aufzubauen als eine Internet-Verlängerung mit ihrer typischen Routing-Struktur. Und wenn der RZ-Bereich auf verschiedene Standorte verteilt ist, wie es sich für ein hochverfügbares RZ gehört, braucht man auch dedizierte Verbindungen zwischen den RZ-Standorten. Anders machen es sogenannte Internetfirmen wie Google auch nicht.

Die obigen Beispiele für nach wie vor erforderliche private Netze erheben keinen Anspruch auf Vollständigkeit. Jedes Unternehmen kann für sich entscheiden, an welchen Stellen und für welche Zwecke noch private Netze erforderlich, sinnvoll und wirtschaftlich gerechtfertigt sind. Doch eins ist klar: angesichts der immer komplexer werdenden Rahmenbedingungen für private Netze und vor dem Hintergrund der in vielen Unternehmen knappen Personalausstattung für die Eigenrealisierung und den Eigenbetrieb der IT gehört jedes private Netz auf den Prüfstand. Nicht nur das Ob, sondern auch das Wie solcher privaten Infrastrukturen ist zu prüfen. Welches Maß an Mandantenfähigkeit ist zum Beispiel erforderlich, wenn außerhalb der besonders geschützten RZ-Bereiche alle Netze als nichtvertrauenswürdig einzustufen sind? Welcher Aufwand für Network Access Control als Mittel der Durchsetzung der Mandantentrennung ist für den dann noch feststellbaren Bedarf an Mandantenfähigkeit eines privaten Netzes einerseits gerechtfertigt und andererseits überhaupt zu verkraften? Wie viel Unified Communications unter zwangsläufiger Einbeziehung von mobilen Geräten kann und sollte man selbst realisieren und betreiben? Und wie sieht diese Lösung aus?

Das sind brennende Fragen, die nicht zuletzt auch die IT-Sicherheit einerseits beeinflussen und andererseits auch unter Berücksichtigung derselben beantwortet werden müssen. Deshalb haben wir unser diesjähriges IT-Sicherheits-Forum unter das Leitmotiv der Post-PC-Ära und ihrer Auswirkungen gestellt.

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Lokale Netze für Einsteiger, 16.04. - 20.04.12 in Aachen

Dieses Seminar vermittelt kompakt und intensiv innerhalb von 5 Tagen die Grundprinzipien des Aufbaus und der Arbeitsweise Lokaler Netzwerke. Dabei werden sowohl die notwendigen theoretischen Hintergrundkenntnisse vermittelt als auch der praktische Aufbau und der Betrieb eines LANs erläutert. Ausgehend von einer Darstellung von Themen der Verkabelung und der grundlegenden Übertragungsprotokolle werden die wichtigen Zusammenhänge zwischen der Arbeitsweise von Switch-Systemen, den darauf aufsetzenden Verfahren und der Anbindung von PCs und Servern systematisch erklärt.

Preis: € 2.490,-- netto

IP-Wissen für TK-Mitarbeiter, 16.04. - 17.04.12 in Bonn

Dieses Seminar vermittelt kompakt und effizient das IP-Wissen, das TK-Mitarbeiter ohne Vorkenntnisse zur Planung und zum Betrieb von IP-basierten Telefonie-Lösungen benötigen. Alle Seminarinhalte werden von einem Referenten mit hoher Praxiserfahrung betreut. Ziel ist dabei bewusst, statt einer umfassenden Theorieschulung gezielt die Aspekte vorzustellen und unter Praxis-relevanten Gesichtspunkten zu beleuchten, die erfahrungsgemäß aus Sicht einer IP-basierten Telefonielösung wichtig sind.

Preis: € 1.590,-- netto

Ausschreibungen im Informations- und Kommunikationsbereich, 17.04.12 in Bonn

Im Fokus des Seminars sind das überarbeitete Vergaberecht und seine Anwendung im Informations- und Kommunikationsbereich. Unter den Bedingungen verschärfter gesetzlicher Auflagen muss die öffentliche Hand im hochkomplexen Bereich der Informations- und Kommunikationstechnologie oft unter großem Zeitdruck europaweite Vergabeverfahren durchführen. Hier ist interdisziplinäre Kompetenz dringend erforderlich. Um Risiken im Vergabeverfahren zu vermeiden, sind die öffentlichen Auftraggeber auf juristische Expertise angewiesen. Um die technischen Ziele im IT- und Kommunikationsbereich (ITK) zu erreichen, brauchen die ausschreibenden Stellen zudem erfahrene Planer, die jahrelange Ausschreibungspraxis mitbringen. Diese kombinierte Expertise ist genau das, was Ihnen das eintägige Seminar der ComConsult Akademie zu Ausschreibungen im Informations- und Kommunikationsbereich bietet.

Preis: € 990,-- netto

Bring Your Own Device - Sichere Integration von mobilen Privatgeräten in die IT-Infrastruktur, 17.04.12 in Bonn

Dieses Seminar analysiert die Gefährdungen und beschreibt die Wege zur sicheren Anbindung privater und fremder mobiler Endgeräte. Verfügbare technische Lösungen werden vorgestellt und Strategien für den Betrieb dieser Lösungen erarbeitet.

Preis: € 990,-- netto

IT-Projektmanagement Kompaktseminar, 23.04. - 25.04.12 in Aachen

Ein Projekt stellt an einen Projektleiter hohe Anforderungen. In diesem Kurs vervollständigen Sie praxisnah Ihre Kenntnisse aus der gesamten Bandbreite des Projektmanagements: Der Kurs umfasst sowohl Administratives, wie Planen und Überwachen des Projekts, als auch Softskills, wie Moderation von Projektsitzungen und Präsentation von Information. Denn die in der Regel nur „lose“ unterstellten Projektmitarbeiter müssen überzeugend auf Basis einer strukturierten Planung geführt werden. Und jede Chance, sich und sein Projekt erfolgreich zu präsentieren, ist zu nutzen!

Preis: € 1.890,-- netto

Interne Absicherung der IT-Infrastruktur, 02.05. - 04.05.12 in Bonn

Bedingt durch Netzkonvergenz, Mobilität und Virtualisierung hat die interne Absicherung der IT-Infrastruktur in den letzten Jahren enorm an Bedeutung gewonnen. Heterogene Nutzergruppen mit unterschiedlichstem Sicherheitsniveau teilen sich eine gemeinsame IP-basierte Infrastruktur und in vielen Fällen ist der Aufbau sicherer, mandantenfähiger Netze notwendig. Dieses Seminar identifiziert die wesentlichen Gefahrenbereiche und zeigt effiziente und wirtschaftliche Maßnahmen zur Umsetzung einer erfolgreichen Lösung auf. Alle wichtigen Bausteine zur Absicherung von LAN, WAN, Endgeräten, RZ-Bereichen, Servern und SAN werden detailliert erklärt und anhand konkreter Projektbeispiele wird der Weg zu einer erfolgreichen Sicherheits-Lösung aufgezeigt.

Preis: € 1.890,-- netto

Virtualisierungstechnologien in der Analyse, 02.05. - 04.05.12 in Bonn

Dieses Seminar liefert einen umfassenden und zugleich detaillierten Einblick in die aktuellen Virtualisierungstechnologien der marktführenden Anbieter. Vom Server über das Netzwerk bis zum Speicher und schließlich auch zum Client werden die Möglichkeiten und Grenzen der Virtualisierungslösungen analysiert. Dabei bleiben auch Sicherheitsaspekte nicht unberücksichtigt. Basis hierfür bilden neben den technischen Grundlagen und Hintergründe die Erfahrungen aus dem Projektalltag sowie die Diskussion mit den Teilnehmern.

Preis: € 1.890,-- netto

RZ-RZ-Kopplung - alles nur eine Frage der Bandbreite?, 07.05.12 in Bonn

Immer mehr Unternehmen sehen sich derzeit damit konfrontiert, ihre Rechenzentrumsdienstleistungen über entfernte Standorte redundant anzubieten. Neben den entsprechenden Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) für Desaster Recovery Konzepte fordert auch die Kundenseite entsprechende Service Level Agreements zur Hochverfügbarkeit ihrer Dienste und Daten ein. In diesem Seminar werden die aktuellen Techniken vorgestellt, technisch erläutert und für die richtige strategische Entscheidung zu einem Gesamtkonzept zusammengeführt.

Preis: € 990,-- netto

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen, 07.05. - 09.05.12 in Bonn

Dieses Seminar behandelt die Projektschritte, Einsatz- und Migrations-Szenarien, einsetzbare Basis-Technologien, Komponenten und erweiterte TK-Anwendungen, Bewertungskriterien für eine TK-Lösung und gibt eine Übersicht über den bestehenden TK-Markt etablierter Hersteller wie Alcatel-Lucent, Avaya, Cisco, Nortel und Siemens aber auch des Newcomers Microsoft.

Preis: € 1.890,-- netto

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze
16.04. - 20.04.12 in Aachen
03.09. - 07.09.12 in Aachen
12.11. - 16.11.12 in Aachen

TCP/IP intensiv und kompakt
07.05. - 11.05.12 in Hamburg
17.09. - 21.09.12 in Düsseldorf

Internetworking
11.06. - 15.06.12 in Aachen
22.10. - 26.10.12 in Aachen

Paketpreis für alle drei Seminare € 6.720,-- netto (Einzelpreise: je € 2.490,-- netto)

ComConsult Certified Trouble Shooter

Trouble Shooting in vernetzten Infrastrukturen
12.06. - 15.06.12 in Aachen
23.10. - 26.10.12 in Aachen

Trouble Shooting für Netzwerk-Anwendungen
26.06. - 30.06.12 in Aachen
04.12. - 07.12.12 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

Session Initiation Protocol Basis-Technologie der IP-Telefonie
18.06. - 20.06.12 in Bonn
29.10. - 31.10.12 in Bonn

Umfassende Absicherung von Voice over IP und Unified Communications
11.06. - 12.06.12 in Köln
01.10. - 02.10.12 in Düsseldorf

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen
07.05. - 09.05.12 in Hamburg
24.09. - 26.09.12 in Bonn
26.11. - 28.11.12 in Bonn

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
16.04. - 17.04.12 in Bonn
10.09. - 11.09.12 in Berlin

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