ComConsult Research

Der Netzwerk Insider

April 2011

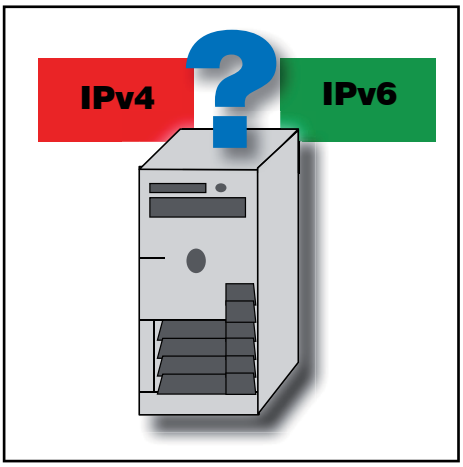
Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

IPv6 - Wenn Dual Stack nicht weiter hilft

von Markus Schaub

NAT bietet sich als logische Lösung für den Übergang zwischen reinen IPv4 Netzen und reinen IPv6 Netzen an. Allerdings ist diese Lösung nicht in allen Fällen trivial und die von IPv4 bekannten Mechanismen sind nicht 1:1 auf alle möglichen Übergänge zwischen Version 4 und 6 übertragbar. Hinzu kommt, dass es immer wieder Fälle gibt, in denen NAT versagt und andere Methoden zum Einsatz kommen müssen, um die Verbindung sicher zu stelle. Dieser Artikel beschäftigt sich mit den neuesten Entwicklungen in der Standardisierung, die eine „sanfte“ Migration auch unter widrigsten Umständen ermöglichen sollen.



NAT

IPv6 soll NAT eigentlich überflüssig machen. Das mag nicht jedem gefallen und ob es am Ende wirklich so kommt, sei einmal dahin gestellt. Doch wird es noch lange dauern, bis wir in einer reinen IPv6 Welt leben und bis dahin macht IPv6 NAT nicht überflüssig, sondern ganz im Gegenteil sogar notwendig. Zwar gibt es eine ganze Reihe von Lösungsansätzen bei der Einführung von IPv6 beide Protokolle parallel zu betreiben, sei es durch Dual Stack oder Tunnel Verfahren, jedoch wird es zwangsläufig zu Situationen kommen, bei denen reine IPv4 Netze mit reinen IPv6 Netzen gekoppelt werden.

weiter auf Seite 14

Zweitthema

Cloud Storage: wer braucht das überhaupt?

von Dr. Behrooz Moayeri

Die Kosten für Massenspeicher sind in den vergangenen zehn Jahren in fast allen Unternehmen kontinuierlich gestiegen, unter anderem weil die durchschnittlich 60 bis 70 Prozent jährliche Wachstumsrate des Speichervolumens in zu kurzen Abständen zum Investitionsbedarf führt.

Auch der Preisverfall im Markt für Massenspeicher, in den letzten Jahrzehnten durchschnittlich 50 bis 60 Prozent pro Jahr, konnte bisher die durch die zu kurzen Lebenszyklen der Speichersysteme verursachten Kostensteigerungen nicht ganz ausgleichen. So ist der Posten Speicher im IT-Budget einer, bei dem man sich auf eines verlassen kann: dass er stetig ansteigt.

weiter auf Seite 23

Aktueller Kongress

IPv6-Forum 2011

ab Seite 11

Geleit

Mobility treibt die Cloud in die Unternehmen

ab Seite 2

Report

Report-Neuerscheinung:

Public und Private Clouds in der Analyse

auf Seite 5

Aktueller Kongress

IT-Sicherheits-Forum 2011

ab Seite 9

Standpunkt

Herausforderung Data Loss Prevention

auf Seite 21

Zum Geleit

Mobility treibt die Cloud in die Unternehmen

Technologie-Statements von ComConsult-Research

Der Einsatz mobiler Endgeräte explodiert. Speziell Tablet-Computer werden auch innerhalb von Unternehmen immer stärker eingesetzt. Dabei geht es nicht nur um die Ablösung oder Ergänzung von Laptops, sondern auch um neue Anwendungsbereiche.

Dies generiert eine Reihe von Fragen:

- Welches mobile Gerät wird das größte Wachstum in den Unternehmen haben?
- Welche Applikationen werden hier speziell angesprochen?
- Warum wird das Cloud-Dienste in die Unternehmen tragen?
- Wie können die damit verbundenen Sicherheitsprobleme gelöst werden?

Fangen wir mit der ersten Frage an. Hier werden wir ohne Frage das größte Wachstum im Bereich der Tablet-Computer sehen. Die große Konkurrenz besteht hier zwischen Apples iPad und Googles Android 3 Honeycomb. Die Entwicklung in den USA zeigte bereits für das erste iPad einen hohen Nutzungsgrad in den Unternehmen, sei es bei Speditionen, im Bildungsbereich oder auch im Gesundheitswesen. Ein leichtes und mobiles Gerät mit einer ergonomischen Bedienung, guter Netzwerk-Einbindung und guter Rechenleistung ist die Basis für viele bisher noch nicht erschlossene Anwendungsbereiche und Prozess-Optimierungen. Unser Statement zu diesem Markt aus der Sichtweise eines Unternehmens (als Privatperson können Sie durchaus zu einem anderen Ergebnis kommen):

Statement 1: Das Apple iPad wird den Markt für Unternehmens-Anwendungen in den nächsten 2 Jahren dominieren

Wir sehen dafür folgende Gründe:

- Die offenere Android-Plattform mag Bastler und Hacker anziehen, in der Praxis hat sie zu einer Fragmentierung des Android-Marktes mit vielen verschiedenen Unterversionen der Geräteanbieter und Provider geführt. Diese Fragmentierung erschwert zum einen die Programmierung von Apps und zum anderen trägt sie das Risiko instabiler Umgebungen. Auch ist damit eine geregelte Upgrade-Strategie nicht umsetzbar, wie deutlich am Chaos der verschiedenen älteren Android-Geräte

zu sehen. Google hat dies erkannt und blockiert den freien Zugang zu Android 3 im Moment, aber es gibt keine veröffentlichte Strategie dazu. Auch verhindert Googles Bekenntnis zu Open Source eine solche Blockade auf Dauer.

- Die offenere Plattform macht das Gerät generell angreifbarer. Einer der Gründe der Stabilität der Apple-Plattformen ist die partielle Nicht-Offenheit und die Bindung an eigene Hardware. Apple hat es erfolgreich geschafft, die Nachteile einer nicht offenen und proprietären Lösung durch seinen App-Store zu kompensieren. Für den Kunden gibt es somit kein Second-Source, aber das gibt es momentan mit der gegebenen Fragmentierung bei Android auch nicht.

- Apple hat mit seinem App-Store einen Vorsprung von mindestens einem Jahr gegenüber Google. Zwar decken die Applikationen, die Google mit 3.0 ausliefert, den Grundbedarf ab, aber gerade die für Unternehmen wichtigen speziellen Applikationen wird es auf lange Zeit nur sehr eingeschränkt geben.

- Das Preis-Leistungs-Verhältnis spricht für die nächsten Monate klar für Apple. Samsungs Reaktion auf die Vorstellung des iPad 2 spricht eine deutliche Sprache.

Dem stehen natürlich die bekannten Nachteile des iPads gegenüber. Aus Unternehmenssicht ist hier zuerst die fehlende Unterstützung von Adobe Flash zu nennen. Speziell im Unternehmensbereich hat Flash eine ernst zunehmende Verbreitung. Zwar hat Adobe gerade einen Flash nach HTML5-Konverter vorgestellt und natürlich ist HTML5 eine zu bevorzugende Alternative, aber man muss auch klar erkennen, dass HTML5 bei weitem nicht den Funktionsumfang von Flash abdeckt.

An dieser Stelle soll auch positiv in Richtung Honeycomb die sehr gelungene Umsetzung von Multi-Tasking angesprochen werden. Apple verweigert sich an dieser Stelle mit Verweis auf die Batterie-Leistung. Tatsächlich hat Google hier mit seiner Lösung einen Vorteil in Richtung Übersichtlichkeit und Zugang zu mehreren offenen Applikationen. Leider löst dies nicht das Problem der Fragmentierung und der fehlenden Applikationen und des fehlenden Contents im Sinne wichtiger Zeitschriften und Bücher.

Damit sind wir bei der Frage der Applikationen, die Tablets für die Unternehmen spannend machen. Hierzu unser Statement:

Statement 2: Wir werden in den nächsten 12 Monaten eine Flut neuer Applikationen für das iPad 2 und speziell für den Unternehmenseinsatz sehen

Der Kreativität und dem Vorstellungsvermögen sind hier keine Grenzen gesetzt. Das iPad ist die wirtschaftliche Basis für die Verbesserung vieler bisher überwiegender manueller Prozesse. Und es hat ein Leistungsniveau in Kombination mit einer Bediensystematik, die den Markt für endlose neue Lösungen öffnet. Das beste Beispiel sind Apples GarageBand und iMovie. Was Apple hier mit diesen Applikationen auf einem mobilen Gerät demonstriert, stellt alles weit in den Schatten, was es bisher in diesem Bereich gegeben hat. Speziell GarageBand zeigt auch, dass es Anwendungen gibt, die man tatsächlich besser auf einem Tablet als auf einem Desktop bedienen kann. Mit Filemaker und Bento wird auch gezeigt, dass komplexere Datenbank-Anwendungen auf einem iPad ausgeführt werden können.

Ein ernstzunehmender Mangel ist die momentan nur eingeschränkte Kompatibilität mit Microsoft Office. Hier bleibt abzuwarten was der Markt (eventuell Microsoft selber?) in den nächsten Monaten liefern wird.

Mobility treibt die Cloud in die Unternehmen

Statement 3: Mobility trägt die Cloud in die Unternehmen

Mobile Geräte und Applikationen müssen in die Unternehmens-Landschaft integriert werden. Gleichzeitig hat speziell das iPad den „Mangel“, konzeptionell auf Cloud-Unterstützung ausgelegt zu sein. Es hat kein offenes eigenes Filesystem, so dass lokal gespeicherte Daten nur für eine Teilmenge der lokal installierten Applikationen zur Verfügung steht, häufig sind die Daten an eine einzige Applikation gebunden, manchmal gestatten Applikationen die Weitergabe an eine beschränkte Menge anderer Applikationen.

Dies hat dazu geführt und ist auch konzeptionell so gewollt, dass die Cloud gezielt mobile Geräte ergänzt. Dabei geht es sowohl um die Bereitstellung von Daten als auch um Applikationen.

Im Bereich der Daten explodieren Dienste wie Dropbox und Box.net. Dropbox hat sich speziell für das iPad zum unverzichtbaren Standard entwickelt. Man kann es mit Berechtigung inzwischen als das inoffizielle Cloud-Filesystem des iPads bezeichnen. Die Nutzerzahl dieser Dienste entwickelt sich exponentiell. Unternehmen, die iPads oder auch andere Tablets zum Einsatz bringen, müssen diese Dienste fest ins Kalkül ziehen. Es geht nur sehr eingeschränkt ohne derartige Dienste. Man spekuliert an dieser Stelle schon lange mit einem entsprechenden neuen Dienst von Apple, der das heutige unhandliche und veraltete MobileMe ablösen soll.

Dabei geht es nicht nur um die Umsetzung eines Filesystems, sondern auch um die Integration mit Desktop und Laptop. Dies geht mittlerweile weit über den Bereich des Filesystems hinaus und umfasst Notiz-Applikationen wie Evernote und Auditorium oder auch Kreativtools wie diverse Mindmapper, Adobe Ideas und Sketchbook. Speziell diese Applikationen zeigen auch, dass ein Tablet in der richtigen Ausführung dem Laptop als Hilfsmittel in Besprechungen überlegen ist.

Ein weiterer wichtiger Bereich ist der aufkommende Markt für HTML5-basierte Cloud-Applikationen. Diese Applikationen sind nicht nur eine ideale Ergänzung von Tablets, sie werden bewusst auch als solche entwickelt. Mit der zunehmenden Reife von HTML5 wird dieser Markt schnell wachsen. Allerdings besteht hier ein steigendes Risiko, dass wichtige Anbieter wie Google und Microsoft doch wieder individuelle Wege mit HTML5 gehen.

Noch einmal im Klartext: der Einsatz mobiler Geräte egal welcher Art ist in Zukunft ohne eine Kombination mit Cloud-Diensten nicht denkbar. Mobile Geräte und Cloud werden von den Anbietern bewusst als Bausteine einer gemeinsamen Architektur entwickelt. Naturgemäß ist das bei Google im Bereich Mail und Dokumentenverarbeitung per se so, aber auch Apple selber geht in diese Richtung.

Statement 4: Damit entsteht eine große Herausforderung für die Sicherheit und damit verbunden auch für den Betrieb solcher Geräte

iPads und auch Androids wurden und werden nicht mit dem Zielmarkt Unternehmen entwickelt (Ausnahme bei Cisco). Dementsprechend werden die verfügbaren Tools für das Provisioning und die Benutzerverwaltung nicht den Bedarf jedes Unternehmens erfüllen. Zwar kann man erwarten, dass sich hier etwas in den nächsten Monaten entwickelt, aber das hier vorliegende Problem ist als sehr groß einzuschätzen. Eine Lösung kann in einer verstärkten Nutzung der Cloud liegen, wenn man dabei Cloud-Dienste nutzt oder entwickelt, die die entsprechenden Anforderungen erfüllen.

Gerade im Bereich Sicherheit entstehen signifikante Risiken. Mobile Geräte können verloren gehen oder gestohlen werden. Apple bietet eine Verschlüsselung der lokal gespeicherten Daten (Hardwarebasiertes 256 Bit AES), ein Remote-Wipe und die Konfiguration einer Reihe von einfachen Policies (Restrictions), konfigurierbare VPN-Lösungen und SSL/TLS und realisiert damit eine einfache Benutzerverwaltung und Sicherheit (Benutzern kann die Änderung von Diensteinstellungen, die Neuanlegung von Email-Accounts und die Neuinstallation von Apps gesperrt werden), aber das wird einigen Unternehmen nicht ausreichen.

Tatsächlich entsteht im Bereich Sicherheit ein Vorteil durch das fehlende Dateisystem des iPad, da Applikationen mit ihren Daten in einer Sandbox laufen (für interessierte Leser wird auf das iPad-Security-Overview-PDF verwiesen: http://images.apple.com/ipad/business/pdf/iPad_Security_Overview.pdf).

Auch hier kann die Konsequenz in der Vermeidung einer lokalen Kopie sicherheitsrelevanter Daten und einer mehr Geräte-neutralen Lösung liegen. Damit sind wir wieder beim Cloud-Dienst angekommen. Die Nutzung von Cloud-Diensten für sicherheitskritische Daten umfasst verschiedene Stufen von Sicherheit:

- In der untersten Stufe verschlüsselt ein Anbieter den Transport und den Speicher, aber mit einem von ihm verwalteten Schlüssel. Auch ist damit unklar, was und wer wirklich Zugang zu den Daten hat. Ein einfaches Sicherheitsbedürfnis für Notizen kann damit abgedeckt werden. (Zitat von Dropbox: To ensure everyone has the ability to view and share files on the web painlessly, Dropbox currently does not support the creation of your own private keys. However, allowing user control over this is something we might consider adding in the future.)

- In der nächsten Stufe kontrolliert das Unternehmen die Verschlüsselung und verwaltet die Schlüssel. (im Prinzip spricht nichts dagegen verschlüsselte disks als Dateien in einem Cloud-Dateisystem zu speichern und von dort zu mounten, allerdings muss das dann

Abbildung 1: Seminar: Public und Private Clouds in der Analyse - Dr. Jürgen Suppan
http://www.comconsult-study.tv/de/Public-und-Private-Clouds-in-der-Analyse::1546:14.html

Mobility treibt die Cloud in die Unternehmen

auch auf der Seite der mobilen Geräte unterstützt werden. Für Desktops und Laptops ist das kein Problem).

- In der höchsten Stufe werden die gesetzlichen Auflagen zur Speicherung von Personendaten in der Cloud erfüllt. Dies erfordert einen relativ komplexen Einzelvertrag mit dem Cloud-Dienstleister und muss für viele der bekannten Anbieter als unrealistisch angesehen werden. Hier ist dann vermutlich eine Private-Cloud-Lösung der einfachere Weg. Diesen Lösungen werden aber die Konnektoren zu den Applikationen auf dem iPad fehlen.

Im Markt scheint mit Bezug auf die Speicherung von Daten in der Cloud die gängige Meinung zu dominieren, die Cloud für unsicher zu halten. Tatsächlich gibt es bei Cloud-Storage Einschränkungen im Sinne der Gestaltbarkeit und Prüfbarkeit der Sicherheit durch ein Unternehmen selber. Auch erschweren rechtliche Probleme die Nutzung von Cloud-Diensten generell. Trotzdem sollte den meisten und speziell kleineren Unternehmen bewusst sein, dass es ihnen schwer fallen wird, das Sicherheitsniveau eines Cloud-Großrechenzentrums mit der eigenen Infrastruktur zu erreichen. Die Kombination dieser Sicherheit mit einer selbst verwalteten Verschlüsselungs-Lösung erreicht durchaus ein ernstzunehmendes Maß an Sicherheit. Ich verweise als Beispiel auf folgende Ausführungen von Amazon: http://aws.amazon.com/articles/1697?_encoding=UTF8&jiveRedirect=1.

Unser Fazit

Mobile Geräte und Tablets werden die Unternehmen in den nächsten zwei Jahren überrollen. Damit werden gleichzeitig auch wichtige Prozessbereiche adressiert, die nun deutlich besser mit IT-Leistungen abgedeckt werden können. Mit dieser Entwicklung gehen erhebliche Herausforderungen an den Betrieb und die Sicherheit dieser Geräte einher. Auch setzt die volle Nutzung des Potenzials der Geräte einen Proaktiven Zugang zu dieser Technologie voraus. Unternehmen sollten nicht warten, bis Mitarbeiter (und Führungskräfte) mit diesen Geräten auftauchen sondern gezielt die Potenziale ausloten und dann die Geräte und damit verbundenen Applikationen in einer gesteuerten und kontrollierten Weise einführen.

Dieses Geleit entstand völlig rückständig auf einem normalen Desktop-PC, der allerdings in den nächsten Wochen durch eine modulare mobile Plattform auf der Basis Thunderbolt abgelöst wird (der Markt kann die Peripherie noch nicht liefern). Allerdings ist mein iPad komplett in die lokale Umgebung durch den Einsatz der angesprochenen Cloud-Dienste integriert.

Ihr
Dr. Jürgen Suppan

Kongress

ComConsult Storage-Forum 2011
13.07. - 15.07.11 in Bonn

Zentraler, im Netzwerk zugreifbarer Speicher steht im Mittelpunkt aller zukünftigen IT-Architekturen. Die technologische Spannweite ist riesig, permanent kommen neue Entwicklungen und Produkte hinzu. Das ComConsult Storage-Forum 2011 analysiert die aktuellen Entwicklungen im Speichermarkt, vergleicht Alternativen und zeigt auf, wo der Weg hingeht.

Die Gründe für den weiter wachsenden Bedarf sind vielfältig:
- Mehr Rechenleistung gestattet die Verarbeitung von immer mehr Daten.
- Auch neue Applikationen und Applikationstypen (Video, Web 2.0/3.0) erzeugen erhebliche Datenmengen.
- Zunehmende Automatisierung (RFID) stellt immer mehr Daten bereit.
- Eine veränderte Risiko- und Rechtssituation erfordert mehr Detail-Daten für eine verbesserte Prognose-Sicherheit.
- Neue Formen der Vermarktung erzeugen neue Daten (Internet).
- Verändertes Kundenverhalten schafft neue Daten zu Kunden-Bedürfnissen und Erwartungen.
- Virtualisierung und Konsolidierung von Servern zentralisiert Daten.

Dies erfolgt parallel zu wesentlichen Änderungen in IT-Technologien und Architekturen, die neue Anforderungen an die Leistung und Qualität von Speicher erzeugen:
- Virtualisierung geht immer mehr weg von der simplen Konsolidierung und hin zur Schaffung neuer Architekturen für Webanwendungen.
- Neue Virtualisierungsverfahen wie vMotion, HA, Desaster Recovery generieren erhebliche Anforderungen an Speicher-Performance.
- Traditionell wurde die Leistung von SAN-Systemen in I/O-Transaktionen pro Sekunde gemessen, mit den neuen Architekturen kommen erhebliche Anforderungen an Bandbreite hinzu.
- Mit Desktop-Virtualisierung entsteht ein erheblicher Mehrbedarf an Speicher.
- Neue Netzwerk-Technologien geben dem Netzwerk Systembus-Charakter und ermöglichen eine Speicher-Einbindung mit bisher unbekannter Leistung.
- Die Entwicklung von SSD-Speicher muss als sehr kritisch angesehen werden, stellt sie doch die traditionelle Formel Lokale Leistung = Zentrale Leistung in Frage. SSD muss zwangsläufig auch im SAN eine Rolle spielen oder es entsteht ein Performance-Loch zur Server-Leistung. Dies generiert neue Probleme im Netzwerk.

Moderatoren: Dipl.-Inform. Matthias Egerland, Dr. Franz-Joachim Kauffels
Preis: € 1.990,-- zzgl. MwSt.

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

Neuer Report

Neuerscheinung März 2011
Public und Private Clouds in der Analyse

Im März 2011 ist die Technologie-Studie "Public und Private Clouds in der Analyse" bei ComConsult Research erschienen.

Cloud-Computing hat sich zu einem derart bedeutenden Hype entwickelt, dass kaum ein Unternehmen daran vorbei kommt, mindestens die möglichen Vor- und Nachteile der Cloud zu evaluieren. Hier setzt dieser Report an, der die Versprechungen der Cloud analysiert und kritisch hinterfragt.

Dieser Report von Dr. Jürgen Suppan und dem Team von ComConsult Research analysiert:

- Was leisten Public Clouds?
- Werden sie sich durchsetzen?
- Wie reif ist die Technologie?
- Wo steht die Private Cloud? Macht sie überhaupt Sinn?
- Welche Vor- und Nachteile bieten diese Technologien?

- Welche Anforderungen an Infrastrukturen entstehen?
- Wer ist wie betroffen?

Die Ergebnisse des Reports sind sehr gemischt. Zum einen können Cloud-Dienste identifiziert werden, die sofort und unmittelbar einen Zugewinn bringen. Der Report verdeutlicht auch, welche IT-Bereiche in Zukunft besonders durch die Cloud beeinflusst werden.

Besonders kritisch wird der Bereich der Private Cloud betrachtet. Der Report findet eine klare Abgrenzung zwischen traditioneller IT und einer Private Cloud. Für Unternehmen, die an Private Cloud-Diensten interessiert sind, wird ein Stufenplan zur Umgestaltung der bestehenden IT aufgezeigt.

Es werden im Report auch kritische Bereiche identifiziert, die mindestens im Moment gemieden werden sollten. Der Report leitet daraus den Bedarf zur Entwicklung eines Unternehmens-spezifischen Cloud-Portfolios, quasi der optimalen Cloud-Dosis, ab. Nutzen Sie diesen hochaktuellen Report, um ihre optimale Cloud-Dosis zu bestimmen.

Kostenlos bei Kongressteilnahme

Sie erhalten diesen Report bei Teilnahme an den Kongressen "ComConsult IPv6-Forum 2011" und "ComConsult Storage-Forum 2011" gratis als Bestandteil der Seminarunterlagen.

Fax-Antwort an ComConsult 02408/955-399

Bestellung
Public und Private Clouds in der Analyse

Ich bestelle den Report
Public und Private Clouds in der Analyse

☐ zum Preis von € 398,-- zzgl. MwSt. und Versand

Bestellen Sie über unsere Web-Seite
www.comconsult-research.de

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

Kongress

ComConsult Storage-Forum 2011 13.07. - 15.07.11 in Bonn

Die ComConsult Akademie veranstaltet vom 13.07. - 15.07.11 ihren neuen Kongress „ComConsult Storage-Forum 2011“ in Bonn. Das Forum war ursprünglich im März geplant und wurde auf den Juli-Termin verschoben.

Zentraler, im Netzwerk zugreifbarer Speicher steht im Mittelpunkt aller zukünftigen IT-Architekturen. Die technologische Spannweite ist riesig, permanent kommen neue Entwicklungen und Produkte hinzu. Das ComConsult Storage-Forum 2011 analysiert die aktuellen Entwicklungen im Speichermarkt, vergleicht Alternativen und zeigt auf, wo der Weg hingeht.

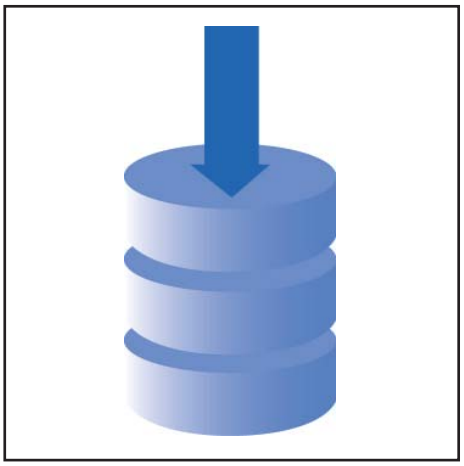
Alle wesentlichen IT-Architekturen werden sich in Zukunft auf zentrale, im Netzwerk zugreifbare Speicher-Lösungen abstützen. Die Bandbreite technologischer Entwicklungen in diesem Bereich, angefangen von neuen IT-Architekturen und hin zu neuen Speicher-Lösungen ist gewaltig. Kombiniert man das mit einem immer weiter wachsenden Datenbestand, dann ergibt dies ein explosives Gemisch:

- Immer mehr Daten müssen beherrscht werden.
- Immer mehr Applikationen hängen von zentralen Speicher-Systemen ab.
- Basis-Funktionen wie Backup/Restore werden zu einem echten Problem.

Die Gründe für den weiter wachsenden Bedarf sind vielfältig:

- Mehr Rechenleistung gestattet die Verarbeitung von immer mehr Daten.
- Auch neue Applikationen und Applikationstypen (Video, Web 2.0/3.0) erzeugen erhebliche Datenmengen.
- Zunehmende Automatisierung (RFID) stellt immer mehr Daten bereit.
- Eine veränderte Risiko- und Rechtssituation erfordert mehr Detail-Daten für eine verbesserte Prognose-Sicherheit.
- Neue Formen der Vermarktung erzeugen neue Daten (Internet).
- Verändertes Kundenverhalten schafft neue Daten zu Kunden-Bedürfnissen und Erwartungen.
- Virtualisierung und Konsolidierung von Servern zentralisiert Daten.

Dies erfolgt parallel zu wesentlichen Änderungen in IT-Technologien und Architek-



turen, die neue Anforderungen an die Leistung und Qualität von Speicher erzeugen:

- Virtualisierung geht immer mehr weg von der simplen Konsolidierung und hin zur Schaffung neuer Architekturen für Webanwendungen.
- Neue Virtualisierungsverfahen wie vMotion, HA, Desaster Recovery generieren erhebliche Anforderungen an Speicher-Performance.
- Traditionell wurde die Leistung von SAN-Systemen in I/O-Transaktionen pro Se--kunde gemessen, mit den neuen Architekturen kommen erhebliche Anforderungen an Bandbreite hinzu.
- Mit Desktop-Virtualisierung entsteht ein erheblicher Mehrbedarf an Speicher.
- Neue Netzwerk-Technologien geben dem Netzwerk Systembus-Charakter und ermöglichen eine Speicher-Einbindung mit bisher unbekannter Leistung.
- Die Entwicklung von SSD-Speicher muss als sehr kritisch angesehen werden, stellt sie doch die traditionelle Formel Lokale Leistung = Zentrale Leistung in Frage. SSD muss zwangsläufig auch im SAN eine Rolle spielen oder es entsteht ein Performance-Loch zur Server-Leistung. Dies generiert neue Probleme im Netzwerk.

Im Gegensatz zur Vergangenheit ist zentraler Speicher als SAN damit nicht mehr nur auf den Datenbank-Bereich beschränkt. Vielmehr muss in Leistung und Bedarf mindestens unterschieden werden nach den Anwendungsbereichen:

- Datenbank- und Mainframe
- File-Services
- Virtualisierung
- Webarchitekturen
- Datensicherung

Das führt direkt zu der Frage, wie sich Anforderungen an Speicher-Technik in Zukunft quantifizieren und messen lassen. Tatsächlich kommen sehr unterschiedliche Kriterien zusammen:

- I/O-Transaktionsrate
- Bandbreite
- Verfügbarkeit
- Speichermenge
- Preis pro TB

Die Kombination sehr unterschiedlicher Anforderungen an den zentralen Speicher aus den verschiedenen Nutzungsbereichen generiert eine Reihe von Problemen oder auch Fragen:

- Handhabung immer größerer Datenmengen
- Aufbau von Hierarchien
- Nutzbarkeit von Bändern
- Backup- und Restore
- Verfügbarkeit
- Performance kontra Preis
- Betrieb zentraler Speicher über Layer-2-Grenzen hinweg
- Umsetzung von Desaster Recovery Konzepten mit großen Datenmengen

Natürlich stehen diesen Problemen und Fragen auch Lösungsansätze gegenüber:

- LifeCycle Management
- Speicher-Virtualisierung
- Deduplizierung • VTL
- Thin Provisioning
- iSCSI/NFS

Diese scheinbar wegweisenden Lösungen generieren aber wieder neue Probleme. Herausragend sind dabei Herstellerabhängigkeit und die Komplexität des Betriebs zu nennen.

Hier setzt unser Forum zur Speicherinfrastruktur 2011 an. Wir analysieren:

- wie sich der Bedarf verändert
- welche Lösungsmöglichkeiten bestehen
- was die verschiedenen Lösungsansätze wirklich bringen
- wie sich die Lösungen in einen handhabbaren Betrieb einbinden lassen

Programmübersicht - ComConsult Storage-Forum 2011

Mittwoch, den 13.07.2011

9:30 bis 11:00 Uhr
Keynote: Vom traditionellen RZ zur Private Cloud
- Cloud Computing: Funktion, Chancen, Risiken
- Entwicklung der Web-Architekturen
- Server-, Speicher- und Netzwerkvirtualisierung
- Entwicklungen bei Netzwerken (Leistung, Latenz, Scale-Out)
- Strukturwandel des RZs
- Hochkonzentrierte Blade-Server: der Host-Phönix?

Dr. Franz-Joachim Kauffels, Unternehmensberater

11:00 bis 11:30 Uhr - Kaffeepause

11:30 bis 12:30 Uhr
Erfahrungen von Unternehmen mit ihrer Speicherinfrastruktur
- Datenwachstum: wie schnell wachsen die Datenbestände?
- Wie ist dem Problem des Datenwachstums beizukommen: mit organisatorischen oder technischen Mitteln?
- Was wird mehr benötigt: Volumen oder Performance?
- Welche neuen Verfahren können genutzt werden, um dem Bedarf an mehr Volumen und Performance gerecht zu werden?
- Abgrenzung zwischen verschiedenen Datenklassen und Speichertypen
- Hochverfügbarkeit der Speicherinfrastruktur
- Herausforderung Datensicherung
- Sinn und Zweck der Speichervirtualisierung
- Wie viel Speichervirtualisierung braucht ein Unternehmen?

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

12:30 bis 14:00 Uhr - Mittagspause

14:00 bis 15:00 Uhr
iSCSI im Rechenzentrum - ein Erfahrungsbericht
- Wie sieht die Grobstruktur des betrachteten RZs aus?
- Welche Anforderungen bestehen seitens der Server beim Zugriff auf den Speicher?
- Welche Aspekte haben die Entscheidung in Richtung iSCSI begünstigt?
- Welche (negativen) Erfahrungen wurden seitens Vattenfall gemacht, als das iSCSI-Netz noch als VLAN über eine gemeinsame Infrastruktur geführt wurde?
- Welche Verbesserungen haben sich ergeben durch die Separierung des iSCSI-Netzes auf dedizierte Hardware?
- Welche Leistungswerte (Durchsatz, IOs, Latenzen) liefert das aktuelle iSCSI-Netz?
- Welche Gründe sprechen aus Sicht von Vattenfall für einen Wechsel auf NFS?

Michael Witschke, Vattenfall IT

15:00 bis 15:30 Uhr - Kaffeepause

15:30 bis 16:30 Uhr
Dateibasierter Speicherzugriff - Erfahrungen aus aktuellen Speicherprojekten
- Wofür eignen sich dateibasierte Verfahren wie NFS, CIFS?
- Was ist neu an NFSv4 und wie wirkt sich das auf die Nutzbarkeit dieses Protokolls als Ersatz von blockbasiertem Speicherzugriff aus?
- Welche Vorteile ergeben sich im Umfeld von NFS bei der Nutzung für Datenbanken oder virtuelle Umgebungen?
- Welche Einschränkungen ergeben sich hierbei?
- In der Praxis erzielbare Leistungswerte: Durchsatz, IOPS, Latenzen
- Wie skaliert eine NFS-Umgebung für Datenbanken und virtuelle Maschinen?
- Gibt es eine Größenordnung (Anzahl Hosts / Anzahl VMs), ab der eine NFS-Umgebung nicht mehr effizient ist?
- Wie gestalten sich Disaster Recovery Szenarien mit NFS?

Michael Albers, Hellweg Data

16:30 bis 17:30 Uhr
Technologische Entwicklungen bei Speichersystemen
- Dauerhaftigkeit von Back-End-Systemen
- Masselose SSDs als neue Speicherklasse
- Weiterentwicklung 3D-SSDs
- Das Netz als Systembus der Virtualisierten Umgebung
- Enterprise Storage Management

Dr. Franz-Joachim Kauffels, Unternehmensberater

Happy Hour ab 18:00 Uhr

Donnerstag, den 14.07.2011

9:00 bis 10:00 Uhr
Konstruktive Sicherheitsaspekte virtualisierter Storage Networks
- Sicherheit in SAN und NAS
- Welche Gefährdungen sind in SAN und NAS relevant?
- Maßnahmen zur Absicherung von SAN und NAS - Elemente einer SAN-Sicherheitsrichtlinie
- Konzepte für eine Zonierung im SAN
- Wann sollte verschlüsselt werden?

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

10:00 bis 11:00 Uhr
Speichervirtualisierung: Steigerung der Flexibilität und Funktionalität oder nur der Komplexität?
- Konzept der Speichervirtualisierung
- Implementierungsvarianten: Inband, Split-Path, Netzwerk-basiert
- Leistungsmerkmale aktueller Lösungen
- Nutzung zur Datenspiegelung zwischen entfernten Standorten

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

11:00 bis 11:30 Uhr - Kaffeepause

11:30 bis 12:30 Uhr
Vereinfachtes Datenmanagement und Kostenreduktion durch Dateivirtualisierung
- Die Herausforderung: exponentielles Wachstum unstrukturierter Daten in traditionellen NAS-Infrastrukturen (NFS, CIFS)
- Die Lösung: Dynamische NAS-Speicherinfrastrukturen durch Dateivirtualisierung
- Funktionsprinzip der Dateivirtualisierung
- Unterbrechungsfreie Datenmigrationen
- Automatische Zuordnung von Daten zu Speicherklassen
- Optimierung von Backups und Kapazitätsverteilung

Dr. Shahriar Daneshjoo, F5 Networks GmbH

12:30 bis 14:00 Uhr - Mittagspause

14:00 bis 15:00 Uhr
Moderne Datensicherung mit VTLs und Disk-2-Disk-Verfahren
- Funktionsweise einer VTL
- Wann ist eine VTL einem allgemeinen Disk-2-Disk-Datensicherungsverfahren vorzuziehen?
- Wie kann eine VTL dabei helfen, aktuelle SLAs gerade im Bereich der Wiederherstellungszeiten einzuhalten?
- Einsatz von Snapshots im Umfeld der Datensicherung
- Datensicherung in virtuellen Umgebungen: LAN-basiert oder LAN-free?
- Möglichkeiten und Grenzen Image- und Datei-basierter Datensicherungen in virtuellen Umgebungen
- Datensicherung mit Bordmitteln der Virtualisierungshersteller und aktuellen Produkten von Drittherstellern

Dipl.-Inform. Matthias Egerland, ComConsult Beratung und Planung GmbH

15:00 bis 15:30 Uhr - Kaffeepause

15:30 bis 16:15 Uhr
Troubleshooting im Fibre Channel

Sebastian Schröder, MEN@NET GmbH

Programmübersicht - ComConsult Storage-Forum 2011

Freitag, den 15.07.2011

9:00 bis 15:00 Uhr
Strategien und Produkte der führenden Hersteller
- Wie sieht die Architektur der Speicherlösung aus?
- Wie skaliert die Leistung des Speichersystems?
- Welche Hochverfügbarkeitsmechanismen besitzt das Speichersystem?
- Wie können Multi-Site Desaster Recovery Szenarien mit dem Speichersystem gelöst werden?
- Welche Vorteile bringt das Speichersystem insbesondere in virtualisierten Umgebungen?

9:00 bis 09:45 Uhr
EMC Symmetrix vMax *Carsten Haak, EMC Deutschland GmbH*

9:45 bis 10:30 Uhr
Fujitsu Eternus
Wolfgang Schenk, Fujitsu Technology Solutions GmbH

10:30 bis 11:00 Uhr - Kaffeepause

11:00 bis 11:45 Uhr
HP Lefthand *Ingo Kraft, Hewlett-Packard Deutschland GmbH*

11:45 bis 12:30 Uhr
IBM XIV *Dirk Vogelsang, IBM Deutschland GmbH*

12:30 bis 13:30 Uhr - Mittagspause

13:30 bis 14:15 Uhr
NetApp FAS/V-Serie *Roger Zink, NetApp Deutschland GmbH*

Anschließende Diskussion mit den Herstellern:
- Wie sieht die Speicherarchitektur der Zukunft aus?
- Welches Speicherzugriffsverfahren wird sich durchsetzen?
- Gehört die Zukunft den SSDs?

15:00 Uhr Ende der Veranstaltung

Inklusive kostenlosem Report bei Kongressteilnahme

Sie erhalten den im März 2011 erschienen Report bei Teilnahme an diesem Kongress gratis als Bestandteil der Kongressunterlagen.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
ComConsult Storage-Forum 2011

Ich buche den Kongress
ComConsult Storage-Forum 2011

☐ 13.07. - 15.07.11 in Bonn
zum Preis von € 1.790,--* zzgl. MwSt.
* gültig bis zum 31.05.2011

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 11

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

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

Aktueller Kongress

IT-Sicherheits-Forum 2011

Cloud, Mobility und Consumerization: kritische Masse für die Informationssicherheit

Wir werden der Cloud nicht entkommen. Die Geschäftsmodelle sind einfach zu attraktiv: Rechenkapazität, Speicherkapazität und Anwendungen nach Bedarf, punktgenau abgerechnet und dies ohne das eigene Rechenzentrum zu belasten. Cloud Computing wird aber zwangsläufig auch Aufbau und Prozesse im Rechenzentrum selbst verändern. Lokale Anwendungen auf virtuellen Servern in der Private Cloud könnten im Bedarfsfall dynamisch durch Rechenkapazität in der Public Cloud unterstützt oder „per Mouse-Klick“ bzw. dynamisch im Rahmen von Load Balancing oder bei Failover in die Public Cloud verlagert werden.

Aus einer Sicherheitsperspektive ist nicht nur die Public Cloud kritisch zu sehen, gerade die eben beschriebene Hybrid Cloud stellt besonders hohe Anforderungen an die Informationssicherheit:

- Welche Geschäftsprozesse sind Cloud-tauglich und welche Sicherheitsanforderungen ergeben sich hieraus?
- Welche Sicherheitsmaßnahmen sind für die verschiedenen Arten von Clouds überhaupt sinnvoll umsetzbar?
- Wie kann mit Daten mit hohem Schutzbedarf in der Hybrid Cloud umgegangen werden?
- Was muss ein Identity Management im Cloud Computing leisten?
- Wie kann Data Leakage Prevention für Daten in Public oder Hybrid Clouds umgesetzt werden?

Insbesondere mobile Nutzer werden unmittelbar von Cloud Computing profitieren. Während für Notebooks als Standardkomponente der IT hier bewährte Sicherheitskonzepte zur Verfügung stehen, bilden Smartphones und Tablets eine vergleichsweise neue Geräteklasse, deren hohes Gefährdungspotential eine genaue Betrachtung erfordert:

- Wie wird sich der Tablet-Markt entwickeln?
- iOS und Android in der Unternehmens-IT: Welche Risiken bestehen?
- Wie können Smartphones und Tablets sicher an die IT-Infrastruktur angebunden werden?
- Virenschutz, Verschlüsselung, Data Leakage Prevention für Smartphones und Tablets: Welche Sicherheitsmaßnahmen sind möglich?
- Was muss ein zentrales Management von Tablets und Smartphones leisten?
- Welche Konsequenzen ergeben sich aus einer App-basierten Architektur für die Informationssicherheit?
- Ist konsequente Virtualisierung die Lösung?

Der verstärkte Einsatz von Tablets und Smartphones auf Basis von Android und iOS im Untenehmen weist auf einen für die Informationssicherheit besonderen Trend hin: die „Consumerization of IT“. Unter diesem Schlagwort werden unterschiedliche Nutzungsformen von Consumer-Produkten in der Enterprise-IT verstanden (z.B. Skype). In diesen Bereich muss auch die Nutzung sozialer Netze im Unternehmen betrachtet werden. Hier wächst der Druck auf die Informationssicherheit solche Produkte freizugeben.

- Wie kann mit Skype und Co. auf eine sichere Weise umgegangen werden?
- Nutzung sozialer Netze durch die Mitarbeiter: Wie kann eine Sensibilisierung erfolgen und welche Richtlinien sollten für den sicheren Umgang festgelegt werden?
- Nutzung sozialer Netze als Informations- und Kommunikationsplattform im Unternehmen: Welche Risiken bestehen und welche Sicherheitsmaßnahmen sollten ergriffen werden?

Cloud Computing, mobile Endgeräte und Consumer-Produkte in der Unternehmens-IT bilden eine kritische Masse für die Informationssicherheit, die wir im ComConsult IT-Sicherheits-Forum 2011 diskutieren werden.

Der Umgang mit dieser kritischen Masse erfordert werkzeuggestützte automatisierte Prozesse, die schnell und adaptiv auf eine sich stetig ändernde Gefährdungslage reagieren können. Grundlage muss ein lebendiger Sicherheitsprozess sein, der Informationssicherheit als Disziplin des Risikomanagements begreift. Wesentliche Elemente eines solchen Information Security Management Systems (ISMS) sind Verwundbarkeits- und Notfallmanagement. Dies sind einige der weiteren Themen, die im ComConsult IT-Sicherheits-Forum 2011 behandelt werden.

Das ComConsult IT-Sicherheits-Forum 2011 ist die zentrale IT-Sicherheits-Veranstaltung des Jahres 2011. 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

IT-Sicherheits-Forum 2011

Ich buche den Kongress
IT-Sicherheits-Forum 2011

☐ 23.05. - 24.05.11 in Königswinter
zum Preis von € 1.790,-- zzgl. MwSt.

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 11

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

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

Programmübersicht - IT-Sicherheits-Forum 2011

Montag, den 23.05.2011

9:30 - 10:30 Uhr
Keynote: Convergence, Consolidation, Cloud und Consumerization - die IT-Sicherheit muss umdenken
- Mobilität, Collaboration und Virtualisierung: Konsequenzen für die Informationssicherheit
- Informationssicherheit trotz maximaler Konsolidierung bei Virtualisierung und Cloud Computing
- Schlüsselelement Mobilität: Tablets und Smartphones als integraler Bestandteil der IT
- Consumerization of IT: Fremdgeräte, Consumer-Geräte, Consumer Software und soziale Netze im Unternehmen
- Seiteneffekte der Konvergenz: Standard-IT-Komponenten in Anlagen, Steuerungen und Maschinen
- Notwendigkeit werkzeuggestützte Prozesse in der Informationssicherheit
- Adaptives Verwundbarkeitsmanagement: Erfassung, schnelle und flexible Reaktion
- Schutz vor Datendiebstahl und -verlust: Content Security, Endpoint Security, DataLeakage Prevention und sichere Netze

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

10:30 - 11:00 Uhr Kaffeepause

11:00 - 12:00 Uhr
IT-Sicherheit und Cloud Computing - ein Widerspruch?
- Was ist Cloud Computing überhaupt?
- Welche Arten von Clouds sind zu unterscheiden?
- Cloud als Ausweichrechenzentrum?
- Welche Geschäftsprozesse sind überhaupt für die Cloud tauglich?
- Welche Sicherheitsanforderungen leiten sich daraus ab?
- Absicherung der Daten in der Cloud: Was ist machbar?
- Identity Management in der Cloud
- Das BDSG und Cloud Computing

Martin Egerter, ComConsult Beratung und Planung GmbH

12:00 - 13:00 Uhr
Sichere Integration von Tablets und Smartphones
- Wie wird sich der Tablet-Markt entwickeln?
- Media Tablets und PC-artige Tablets: ein großer Unterschied für die Informationssicherheit
- Sichere Anbindung von Tablets und Smartphones an die IT-Infrastruktur
- Konsequenzen einer App-basierten Architektur auf die Informationssicherheit
- iOS und Android in der Unternehmens-IT: Risiken und Maßnahmen
- Zentrales Management von Tablets und Smartphones
- Ist konsequente Virtualisierung die Lösung?

Dr. Frank Imhoff, ComConsult Beratung und Planung GmbH

13:00 - 14:15 Uhr Mittagspause

14:15 - 15:00 Uhr
Consumer Software und soziale Netze im Unternehmen
- Nutzung sozialer Netze durch die Mitarbeiter: Sensibilisierung und Richtlinien für den sicheren Umgang
- Nutzung sozialer Netze als Informations- und Kommunikationsplattform im Unternehmen: Risiken und Sicherheitsmaßnahmen
- Sicherer Umgang mit Skype und Co.

Dr. Frank Imhoff, ComConsult Beratung und Planung GmbH

15:00 - 15:45 Uhr
Netzwerk-Sicherheit
- Sicherheitszonen und Mandantenfähigkeit im LAN
- NAC in der Projektpraxis
- Desktop-Virtualisierung: Brauchen wir noch Sicherheit im LAN?
- Sicherer Umgang mit Fremdgeräten
- Verschlüsselung in LAN und WAN: Anforderungen und Techniken
- Wo steht MACsec und was leistet IEEE 802.1X-2010?

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

15:45 - 16:15 Uhr Kaffeepause

16:15 - 17:00 Uhr
Angriff auf die Leittechnik - Stuxnet und die Konsequenzen
- Rückblick: Funktionsweise und Schadfunktion des Stuxnet-Wurms
- Derzeitiger Stand: Systeme gepatcht -Lücken geschlossen?
- Aktuelle Schwachstellen in der Prozessleittechnik: Gefährdung durch Nachahmungstäter
- Ausblick: Konsequenzen für Leittechnik-Betreiber und Hersteller

Dr. Stephan Beirer, GAI NetConsult GmbH

17:00 - 17:45 Uhr
Praktische Herangehensweise an BCM Projekte
- Überblick zum Notfallmanagement
- Notfallszenarien und deren Bewältigung
- Durchführung und Dokumentation von Notfalltests
- Tooleinsatz im Notfallmanagement

Holm Diening, GAI NetConsult GmbH

ab 18:00 Uhr Happy Hour

Dienstag, den 24.05.2011

9:00 - 9:45 Uhr
Sicherheitsmanagement und Risikomanagement - Theorie, Praxis und Werkzeuge
- Governance, Risk und Compliance: Grundlagen zum Informationssicherheits-/IT-Risikomanagement
- Inhalte eines Information Security Management Systems (ISMS)
- Aufgaben und Schnittstellen im Informationssicherheitsmanagement
- Typische Probleme bei der Umsetzung des ISMS
- Werkzeuge zur Unterstützung des Informationssicherheits-und Risikomanagements: Funktionsweise, Einsatzzwecke, Mehrwert, Herausforderungen, Marktüberblick, Vorgehensweise bei der Produktfindung und Einführung

Stefan Strobel, Cirosec GmbH

9:45 - 10:30 Uhr
ISMS-Kernprozess Verwundbarkeitsmanagement
- Vorgehensweisen zur Identifikation / Bewertung von Verwundbarkeiten, Entwicklung und Umsetzung von Maßnahmen
- Notwendige Prozesse und Schnittstellen zu Change Management und Incident Management
- Verwundbarkeitsdatenbanken
- Scanner und andere Werkzeuge

Andreas Meder, ComConsult Beratung und Planung GmbH

10:30 - 11:00 Uhr Kaffeepause

11:00 - 11:45 Uhr
Data Loss Prevention: Methoden und Werkzeuge
- Techniken zur Überwachung der Kommunikation
- Agentenbasierte DLP-Lösungen - mehr als Überwachung der Schnittstellen!
- Herangehensweise und Probleme in der Praxis
- Welche Daten sind überhaupt zu schützen? DLP und Datenklassifikation
- Zwischen DLP, DRM und IRM: Überschneidungen und Abgrenzung
- Was leisten die auf dem Markt verfügbaren Produkte?

Stefan Strobel, Cirosec GmbH

11:45 - 12:30 Uhr
Borderless Network Security
- Unified Computing: Warum Server und Netz zusammen wachsen
- Adaptive Sicherheit durch Kooperation von Sicherheitskomponenten und Netz
- Content Security, E-Mail und Web-Sicherheit: Schnelle und flexible Antwort auf sich ändernde Gefährdungen
- Endpoint Security und NAC bei uneingeschränkter Mobilität
- TrustSec: Sicherheit im Netz vom RZ bis zum Endgerät

N.N., Cisco Systems

12:30 - 13:45 Uhr Mittagspause

13:45 - 14:30 Uhr
Schutz unternehmenskritischer Applikationen durch Advanced Application Delivery
- Beitrag von Load Balancern und L4-7 Switches zur IT-Sicherheit
- Application Layer Firewalls: Notwendigkeit und Technik
- Authentisierung, feingranulare Zugangskontrolle und -berechtigung

Frank Thias, F5 Networks

14:30 - 15:30 Uhr
Sicherheitsaspekte bei IPv6
- IPv6: Neuerungen und Gefährdungslage
- IPv6-Basismechanismen und Standarddienste: Kurzeinführung und Hinweise auf Angriffspunkte
- Ping Sweep für IPv6 - Sicherheitsrelevanz
- Secure Neighbor Discovery SEND
- Firewalls und IPv6
- MS Direct Access unter Sicherheitsgesichtspunkten
- SOHO und Sicherheit bei IPv6-Einführung

Oliver Flüs, ComConsult Beratung und Planung GmbH

Ende der Veranstaltung 15:30 Uhr

Neuer Kongress

ComConsult IPv6-Forum 2011

Die ComConsult Akademie veranstaltet vom 09.05. - 11.05.11 ihren neuen Kongress „ComConsult IPv6-Forum 2011“ in Königswinter.

An dem Thema IPv6 kommt man heute kaum vorbei. Selbst die Massenmedien berichten mal mehr, mal weniger korrekt darüber. Doch was wie ein einfacher Wechsel von einem Protokoll zu einem anderen aussieht, entpuppt sich bei genauerem Hinsehen fast schon als Paradigmenwechsel. IPv4 hat unsere IT-Welt so lange dominiert, dass es als unveränderlich hingenommen wurde. So ist es nicht verwunderlich, dass seine Bedeutung mit der Zeit weit über die eines reinen Transportprotokolls hinaus gewachsen ist. Wir finden IP Adressen heute in Protokollen höherer Schichten, in Anwendungen und in Sicherheitskonzepten wieder. IP ist so tief in unserer gesamten IT-Architektur verwurzelt, dass ein einfaches Versionsupgrade von 4 auf 6 schlicht unmöglich geworden ist.

Eben so unmöglich ist es allerdings für Betreiber und Planer das Thema zu ignorieren. Das Projekt „Aussitzen“ funktioniert nicht. Betriebssysteme von Microsoft und anderen Herstellern haben den IPv6 Stack per Default aktiviert und ohne es zu wissen, wird in vielen Netzen heute bereits zum Teil mit IPv6 kommuniziert. Erste Probleme in den Bereichen Betrieb und Sicherheit sind bereits aufgetaucht. Eine „sanfte Migration“, wie sie der Dual Stack zu versprechen scheint, wird in den meisten Fällen nicht möglich sein.

Weitere Gründe für eine sorgfältige Planung der Migration sind:

- Nicht jede Software und Hardwarekomponente wird nach IPv6 migriert werden können. Für diese Fälle müssen Konzepte für den Betrieb und die Ablösung entwickelt werden.

- In anderen Fällen macht der Wechsel Upgrades der Firm- oder Software erforderlich. Nicht immer gewährleisten diese den gesamten Leistungsumfang der IPv4 Versionen. Gerade bei Firewalls gibt es hier noch erhebliche Defizite.

- NAT ist oft integraler Bestandteil von Sicherheitskonzepten. Doch NAT bringt auch Probleme mit sich. Mit IPv6 kann grundsätzlich darauf verzichtet werden. Wie sieht ein Sicherheitskonzept ohne NAT aus und ist das wirklich sinnvoll?

- Cloud-Computing und Virtualisierung sind neben IPv6 zu Zeit die Schlagworte der IT. Für alle drei Technologien gilt, dass sie sich aktuell in einem dynamischen Entwicklungsstadium befinden. Ihre Einführung muss somit aufeinander abgestimmt werden.

Hier setzt unser ComConsult IPv6-Forum 2011 an. Es greift diese Fragen strukturiert auf und zeigt den optimalen Weg nach IPv6 auf. Im Einzelnen beschäftigt sich das IPv6 Forum 2011 mit folgenden Fragen:

- Was ändert sich in der Konzeption bei IPv6?
- Welche Migrationskonzepte gibt es und wie sind sie zu bewerten?
- Welche praktischen Erfahrungen wurden in Projekten bereits gesammelt?
- Was ändert sich beim Troubleshooting?
- IPv6 und Sicherheit: Was gilt es zu beachten?
- Mobiles Arbeiten mit IPv6: was machen iOS, Android und Co?
- Was tut sich bei den Providern?
- Jenseits der Netzhardware und Betriebssysteme: wo lauern Probleme bei Soft- und Hardware und wie kann damit umgegangen werden?
- Wie stellt sich IPv6 aus der Sicht des Adress-Managements dar?
- Wie ist Stand der Unterstützung durch die Netzwerk-Hersteller?

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.

Programmübersicht - IPv6-Forum 2011

Montag, den 09.05. 11 - „Motivation und Grundlagen“

9:30 bis 11:00 Uhr
IPv6-Vorbereitung: Warum, wann und wie?
- Warum muss man sich schon jetzt auf IPv6 vorbereiten?
- Wie lange kann die Umstellung noch vermieden werden?
- Was sich mit IPv6 ändert
- Anforderungen an das Netz
- Sinnvolle Bestandteile eines IPv6-Projektes
- Erfahrungen eines Umstellungs-Projektes

Markus Schaub, ComConsult Research Ltd., ComConsult-Study.tv

11:00 bis 11:30 Uhr - Kaffeepause

11:30 bis 12:45 Uhr
Was ist IPv6: Von der Adresse zu neuen Betriebsformen
- Neue Adressen, Adresstypen und Adressdarstellung
- Wie funktioniert der Parallelbetrieb IPv4 und IPv6?
- Wie wirkt sich IPv6 auf bestehende IP-Subnetzstrukturen aus?
- IPv6-Routing
- Die neue Rolle des Routers
- Anforderungen an Komponenten
- Migrations-Varianten

Dipl.-Inform. Petra Borowka-Gatzweiler, UBN

12:45 bis 14:15 Uhr - Mittagspause

14:15 bis 15:30 Uhr
IPv6-Konfigurationsparameter und Entscheidungen aus betrieblicher Sicht
- Welche Art der Adresszuteilung ist wann sinnvoll? (Autoconfiguration, Autoconfiguration mit ergänzendem DHCP, Stateful DHCP)
- Privacy options: (Warum? Ansätze? Was setzt man wo/wann ein?)
- Vorteil-Nachteil-Betrachtung zu den Alternativen
- Rolle der Netzwerk-Komponenten bei der Konfigurationsverwaltung
- Umsetzung und produktspezifische Anteile am Beispiel Windows 7

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

15:30 bis 16:00 Uhr - Kaffeepause

16:00 bis 16:45 Uhr
IPv6 @ Bosch
- Vorgehen (Vorgeschichte, Projektplanung, Pilot)
- Erfahrungen (LAN, WAN, Internet-Zugang, Adresskonzept, DHCP, DNS, autoconfiguration)
- Fazit

Anja Moog-Lölkes, Robert Bosch GmbH

16:45 bis 17:30 Uhr
Trouble-Shooting in IPv6-Umgebungen
- Was ist anders? • Erfahrungswerte • Empfehlungen

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

ab 18:00 Uhr - Happy Hour

Programmübersicht - IPv6-Forum 2011

Dienstag, den 10.05.11 - „Sicherheit, UC, Mobiles Arbeiten“

9:00 bis 10:00 Uhr
IPv6-Readyness: Funktioniert Interoperabilität?
- Wer garantiert IPv6-Readyness?
- Wie laufen Interoperabilitätstests ab?
- Wie vertrauenswürdig sind die Angaben?
- Komponentensituation im Netzwerkbereich

Dipl.-Inform. Petra Borowka-Gatzweiler, UBN

10:00 bis 10:45 Uhr
IPv6 Migrationsszenarien im TK- und UC- Lösungsgeschäft
- Besonderheiten im Telekommunikationsumfeld
- Portfoliobetrachtungen vom Client bis zum Server
- Planung und Projektmanagement von komplexen Projekten

Michael Tietsch, Siemens Enterprise Communications GmbH und CoKG

10:45 bis 11:15 Uhr - Kaffeepause

11:15 bis 12:45 Uhr
IPv6 und mobiles Arbeiten
- IPv6 im Internet und IPv6 im Intranet - zwei unterschiedliche Anforderungen
- IPv6 in Wireless LANs
- Performance-Aspekte für mobiles Arbeiten
- Wie lassen sich Android, iPhone & Co. integrieren?
- Vorführung, Erfahrungen aus Test-Installationen

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

12:45 bis 14:00 Uhr - Mittagspause

14:00 bis 15:30 Uhr
Sicherheitsaspekte bei IPv6
- Gefährdungslage: Ansätze für Angriffe auf IPv6-Kommunikation
- IPsec unter IPv6
- Security in IPv6-Spezifikationen: Basismechanismen und Standarddienste
- Secure Neighbour Discovery SEND
- Firewalls, IPS und Security Gateways und IPv6
- VPN und IPv6
- Sicherheitsaspekte von MS Direct Access
- Die zukünftige Rolle von NAT

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

15:30 bis 16:00 Uhr - Kaffeepause

16:00 bis 17:00 Uhr
IPv6 in virtuellen Umgebungen
- Sprunghafter Anstieg des IP-Adressbedarfs: Nach den PCs und IP-Telefonen kommen die Thin-Clients mit virtuellen Desktops
- Wie weit geht die IPv6-Fähigkeit heutiger Virtualisierungslösungen?
- Welche Herausforderungen bringen IPv6-nutzende Betriebssysteme in virtuellen Umgebungen?
- Müssen virtuelle Switches IPv6-fähig sein?
- Welche Anforderungen bringt IPv6 für IP-basierte Speicherprotokolle (iSCSI, NFS)?
- Layer-3-Grenzen überschreitende Virtualisierungscluster mittels Microsoft Hyper-V, Windows Server Failover Clustering (WSFC) und IPv6

Dipl.-Inform. Matthias Egerland, ComConsult Beratung und Planung GmbH

17:00 bis 17:45 Uhr
L4/7-Switching als Hilfsmittel für die Migration zu IPv6
- Application Delivery Controller – mehr als nur Loadbalancer
- Application Layer Gateway, Mittler zwischen IPv4/IPv6
- Beispiel: Heterogene IPv4/IPv6 Welten im Service Provider Umfeld
- Weitere Anforderungen und Rahmenbedingungen einer Gesamtlösung

Ralf Sydekum, F5 Networks GmbH

Mittwoch, den 11.05.11 - „Marktsituation“

9:00 bis 9:45 Uhr
IPv6 für Kunden der Deutschen Telekom
- Warum benötigen wir IPv6 und warum führen wir IPv6 ein?
- Wie führen wir IPv6 ein und wie können Kunden IPv6 nutzen?
- Herausforderungen im Enterpriseumfeld
- Was kommt nach der IPv6 Einführung? • Company Connect und IPv6

Karsten Fleischhauer, Deutsche Telekom Netzproduktion GmbH

9:45 bis 10:30 Uhr
IPv6-Unterstützung im Büroumfeld
- Welche Versionen der Betriebssystem sind „IPv6 Ready“ und was bedeutet das?
- Welche Erfahrungen gibt es bei Windows, Linux und MacOSX?
- In welchem Umfang sind Standard-Büroanwendungen und Personal Firewalls schon IPv6-kompatibel?
- Welche Ansätze gibt es für nicht IPv6-“portierwilligen“ Lösungen?
- Wie ist der Stand bei Druckern und Multifunktionsgeräten?

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

10:30 bis 11:00 Uhr - Kaffeepause

11:00 bis 11:45 Uhr
Cisco IPv6 im Enterprise-Netzwerk
- Readiness IPv6: was kann die HW/SW heute?
- Roadmap IPv6: wie geht‘s weiter?
- Herausforderung IPv6: wo sind die Ecken und Kanten?

Gerd Pflüger, Cisco Germany GmbH

11:45 bis 12:45 Uhr
IPv6 Infrastruktur Management
- Integration von IPv6 mit DDI

Silvia Hagen & Frey Khademi, BlueCat Networks

- IPv6 aus der Perspektive von IP Address Management (IPAM)

Thomas Erhardt, n3k Informatik GmbH

12:45 bis 14:00 Uhr - Mittagspause

14:00 bis 14:45 Uhr
Projekterfahrungen mit IPv6
- Einführung von IPv6 beim BMI *Randi P. Korff, Bundesverwaltungsamt*

14:45 bis 15:30 Uhr
Diskussionsrunde: Wie ausgereift ist die Technologie?
- Sind Markt und Produkte wirklich reif für die Umstellung?
- Machen die bekannten Migrationsverfahren Sinn?
- Wie tragfähig ist ein Parallelbetrieb?
- Wie groß sind die Sicherheitsrisiken?

15:30 Uhr Ende der Veranstaltung

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
ComConsult IPv6-Forum 2011

Ich buche den Kongress
ComConsult IPv6-Forum 2011

☐ 09.05. - 11.05.11 in Königswinter
zum Preis von € 1.990,-- zzgl. MwSt.

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 11

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

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

ComConsult-Study.tv

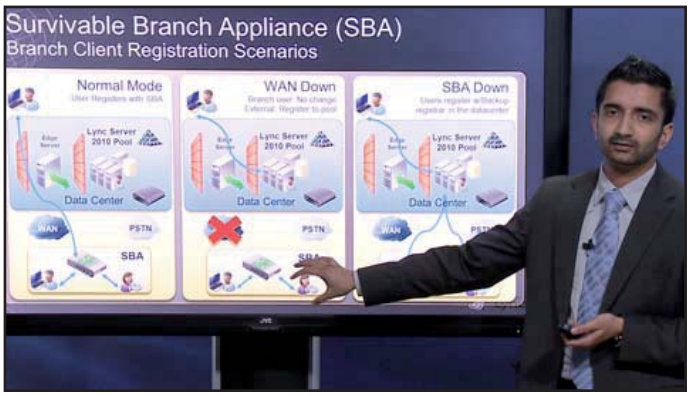
Aktuelle Neuerscheinungen bei ComConsult-Study.tv

Themenbereich: Unified Communications

Seminar: Microsoft Lync: der Client
Referent: **Sven Thimm**
Zeit: 00:34:40 gesamt
Preis: Kostenlos

Microsoft hat mit dem Lync-Client die Messlatte für die Konkurrenz sehr hoch gelegt. Dieses Seminar mit Sven Thimm von Microsoft beschreibt, wie der Client arbeitet und wie er in seine Umgebung eingebunden ist.

Themenbereich: Unified Communications
Microsoft Lync:
Architektur und Hochverfügbarkeitsszenarien
Referent: **Rajesh Vanniamparampil**
Zeit: 00:36:38
Preis: Kostenlos



Dieses Video beschreibt die Architektur des Microsoft-Lync-Servers in den verschiedenen Ausbaustufen. Basierend auf diesen Erklärungen werden die verschiedenen Hochverfügbarkeits-Optionen vorgestellt.

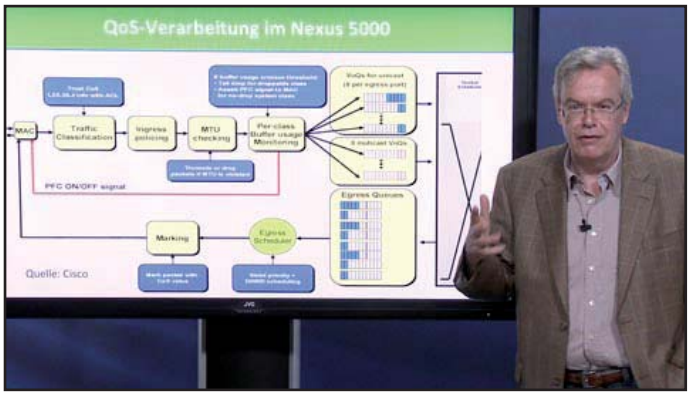
Themenbereich: Web

Seminar: Streaming-Server
Referent: **Dipl.-Inform. Ulrike Häßler**
Zeit: 00:16:23 gesamt
Preis: Kostenlos mit Abo

Dieses Seminar erklärt, welche Alternativen zum Aufbau eines Video-Streaming-Servers auf einem (Web-) Server existieren.

Themenbereich:Desktop, Server, Speicher

Low Latency Netzwerke
Referent: **Dr. Franz-Joachim Kauffels**
Zeit: 00:38:00
Preis: Kostenlos mit Abo



Investitionsschutz im Rechenzentrum ist identisch mit dem Aufbau von Low Latency Netzwerken. Diese sind die Basis für zukunftssichere Server- und Speicher-Architekturen im Netzwerk. Dr. Kauffels erklärt in diesem Video die Hintergünde von Low Latency Netzwerken und geht dabei exemplarisch auf einige wichtige Produkte aus diesem Bereich ein.

Zweitthema

IPv6 - Wenn Dual Stack nicht weiter hilft

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.

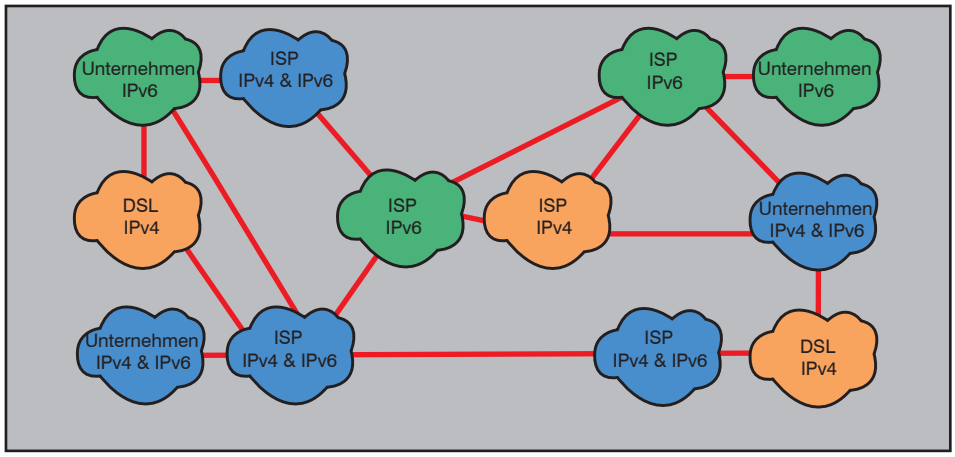


Abbildung 1: Netzstruktur des Internets während der Migration

IPv6 ist über 15 Jahre alt und die Idee des sanften Überganges war es, dass man zunächst in sämtlichen Backbones beide IP Versionen parallel betreibt und dann mit der Migration der Endgeräte und Server beginnt, die ihrerseits beide Versionen beherrschen. Ist die Umstellung komplett, kann man das alte Protokoll abschalten. Ein schöner Traum, aber eben auch nur das: ein Traum.

Die Realität ist eine andere. Die IPv4 Adressen gehen grade so plötzlich dem Ende entgegen wie Weihnachten jedes Jahr plötzlich vor der Türe steht. Die Zeit für solch eine sanfte Migration besteht nicht mehr. Betrachtet man ganz nüchtern die Situation des Internets, war diese wohl auch nie wirklich wahrscheinlich: das Internet und daran angeschlossene Netzwerke bestehen aus zu vielen unterschiedlichen Netzen und Betreibern in zu vielen Ländern mit zu unterschiedlichen finanziellen Mitteln. Die Umstellung auf IPv6 fähige Hardware kostet jedoch viel Geld. Aber auch für Deutschland darf bezweifelt werden, dass private DSL-Anschlüsse respektive die daran angeschlossenen Heimnetze innerhalb von zwei bis drei Jahren komplett auf IPv6 umgestellt werden können: Man bedenke einfach mal, wie viele Geräte in Haushalten heute schon IP nutzen, die selten ausgetauscht werden. Als Stichworte seien hier Blue-Ray Player, Satelliten-Receiver und Spielekonsolen genannt. Geräte, die häufig ein langes Leben in einem Haushalt haben. Auf der anderen Seite wird mit dem Ende verfügbarer IPv4 Adressen zunehmend Netze geben, die ausschließlich auf IPv6 beruhen. Der Übergang von Version 4 auf Version 6 wird also nicht „sanft“ werden, aber trotzdem muss er für den User transparent sein.

Um diesem Problem zu begegnen, hat sich vor geraumer Zeit bei der IETF eine Arbeitsgruppe dieser Thematik gewidmet und Lösungen erarbeitet. Aktueller Stand ist, dass die wichtigsten Bestandteile dieser Lösung darauf warten vom Draft zum RFC erhoben zu werden. Es lohnt sich also, diese genauer unter die Lupe zu nehmen, da die Standards stabil sind und der aktuelle Stand der Migration weit genug fortgeschritten ist, dass entsprechende Probleme auch bereits auftauchen.

IPv4-Embedded IPv6 Adressen

Eine zentrale Rolle für den Übergang von IPv4 in IPv6 Netze und umgekehrt haben die IPv4-Embedded IPv6 Adressen. Dabei handelt es um ein Verfahren, mittels dessen IPv4 Adressen eindeutig in IPv6 Adressen abgebildet werden. Häufig liest man in diesem Zusammenhang von 'IPv4-compatible' IPv6 Adressen (::ffff:0:0/96) und 'IPv4-mapped' IPv6 Adressen (::/96). Beispiele sind ::ffff:192.0.1.1 bzw. ::192.0.1.1. Letztere sind jedoch von der IETF wieder zurück gezogen worden und müssen nicht mehr unterstützt werden, erstere sind für den Gebrauch im Zusammenhang mit Dual Stacks gedacht.

Im Zusammenhang mit NAT werden zwei neue Adressen für die Abbildung von IPv4 Adressen in IPv6 Adressen eingeführt:

Well-Known Präfix: 64:ff9b::/96

Das „Well-Kown-Präfix“ wird als Netzwerk-Präfix genutzt und die IPv4 Adresse als Host-Anteil. Ein Beispiel zeigt Tabelle 1.

Bei der Schreibweise ist zu beachten, dass es sich um eine alternative Schreibweise für IPv4-Embedded IPv6 Adressen handelt und äquivalent zu 64:ff9b::95E0:710B ist.

Der Vorteil des Well-Known-Präfix ist, dass man beim Troubleshooting solche Adressen leicht identifizieren kann. Der Nachteil

Well-Known Präfix	IPv4 Adresse	IPv4-Embedded IPv6 Adresse
64:ff9b::/96	149.224.116.11	64:ff9b::149.224.113.11

Tabelle 1: Well-Known-Präfix

IPv6 - Wenn Dual Stack nicht weiter hilft

	IPv6 Adresse															
Präfix-Länge	0	8	16	24	32	40	48	56	64	72	80	88	96	104	112	120
32	Präfix				(32)				u	suffix						
40	Präfix					(24)			u	(8)	suffix					
48	Präfix						(16)		u	(16)						
56	Präfix							(8)	u	(24)			suffix			
64	Präfix								u	(32)				suffix		
96	Präfix												(32)			

Tabelle 2: Bildungsschema für IPv4-Embedded IPv6 Adressen

ist, dass man ein weiteres Präfix im Netz hat, das sich nicht unmittelbar in das eigene Adresskonzept einfügt und somit beim Routing beispielsweise nicht aggregiert werden kann.

Und eine Einschränkung gibt es für die Nutzung auch: das Well-Known-Präfix darf nur im Zusammenhang mit global vergebenen IPv4 Adressen genutzt werden, also keinesfalls mit den in RFC 1918 spezifizierten privaten IP Adressen.

Trotz dieser beiden Einschränkungen gibt es Anwendungsfälle, die die Nutzung nahe legen. Auf diese Fälle wird später noch eingegangen.

Network-Specific Präfix

Um die Restriktionen des Well-Known Präfix zu umgehen, kann man auch das eigene Präfix nutzen. Doch auch das hat seine Tücken. Zwar läge es auf der Hand, es genau so zu bilden wie beim Well-Known Präfix, jedoch erlaubt der Standard hier mehr Möglichkeiten. Das macht zwar einerseits die Integration in ein eigenes Netzwerk-Adress-Konzept einfacher, andererseits wird die Anzahl der Möglichkeiten jedoch unübersichtlicher. Im Troubleshooting Fall wird das in Zukunft für so manches Kopfzerbrechen sorgen, da die Adressen nicht mehr in jedem Fall einfach als IPv4-Embedded IPv6 Adressen zu erkennen sind.

Konkret sind die in Tabelle 2 dargestellten Möglichkeiten erlaubt.

Die Tabelle zeigt das Bildungsschema für IPv4-Embedded IPv6 Adressen mit eigenem Netzwerk Präfix. Die Zahlen in Klammern sind jeweils die Anzahl der Bits der abgebildeten IPv4 Adressen. Die Bildungsvorschriften lauten wie folgt:

- Das Präfix ist das eigene Netzwerk-Präfix, respektive das selbst gewählte Präfix für IPv4-Embedded IPv6 Adressen. Zulässig sind nur 32, 40, 48, 56, 64 und 96 Bit lange Präfixes.

- Die IPv4 Adresse beginnt unmittelbar nach dem Präfix. Falls nötig, werden die fehlenden Bits ab dem 72. Bit ergänzt (siehe nächster Punkt).

- Die Bits 64-72 (u) sind reserviert. Um die Kompatibilität Host Adressen zu gewährleisten, müssen diese Bits auf 0 gesetzt werden.

  Das gilt übrigens auch für das 96-Bit lange Präfix. In diesem Fall wird empfohlen, ein 64 Bit langes Präfix festzulegen und die Bits 64 bis 95 Bit mit Nullen aufzufüllen.

- Das Suffix wird zur Zeit nicht genutzt und könnte höchstens in Zukunft eine Bedeutung bekommen, bis dahin werden alle Bits auf Null gesetzt.

Präfix-Länge	Präfix	IPv4 Adresse	IPv4-Embedded IPv6 Adresse
32	2001:db8::	149.224.113.11	2001:db8:95e0:710b::
40	2001:db8:100::	149.224.113.11	2001:db8:195:e071:b::
48	2001:db8:123::	149.224.113.11	2001:db8:123:95e0:71:b00::
56	2001:db8:123:400::	149.224.113.11	2001:db8:123:495:e0:710b::
64	2001:db8:123:456::	149.224.113.11	2001:db8:123:456:95:e071:b00::
96	2001:db8:123:456::	149.224.113.11	2001:db8:123:456::149.224.113.11

Tabelle 3: Beispiel für IPv4-Embedded IPv6 Adressen

Tabelle 3 zeigt ein Beispiel für die erlaubten Varianten von IPv4-Embedded IPv6 Adressen.

Es ist offensichtlich, dass für Unternehmensnetze nur die Varianten mit einem 48 Bit Präfix und länger in Frage kommen, da nur wenigen kürzere Präfixes zugewiesen werden dürften.

NAT64

Häufig liest man die Begriffe NAT46 und NAT64, damit ist eine Übersetzung von einem IPv4 Netz in ein IPv6 Netz bzw. umgekehrt gemeint. Die erste Zahl gibt dabei an von wo ein Paket kommt, die zweite wo es hin will. Die Autoren der RFCs nutzten diese Unterscheidung für NAT so nicht, sondern sprechen von "stateful" und "stateless", was nicht die Richtung, sondern die Art der Übersetzung adressiert. Doch dazu später mehr. Das Problem sieht nämlich nur auf den ersten Blick symmetrisch aus. Wegen der erheblich größeren Anzahl von IPv6, kann zwar jede V4-Adresse in V6 abgebildet werden, umgekehrt ist das jedoch unmöglich.

Zunächst der einfachere Fall: Jemand aus einem reinen IPv6 Netz versucht auf einen Server in einem reinen IPv4 Netz zuzugreifen (vgl. Abbildung 2).

Mittelfristig wird es zu dieser Situation kommen. Spätestens wenn die IPv4 Adressen aufgebraucht sind, wird es zunehmend Fälle geben, in denen es gar nicht anders geht.

Für diesen Fall bietet NAT eine Lösung, die auf einer eindeutigen Abbildung der IPv4 Adresse in eine IPv6 Adresse beruht. Welche Adressen dafür genutzt werden und wie das funktioniert, wurde bereits oben erläutert.

Der IPv6-Client baut eine Verbindung zu dem IPv4-Server wie folgt auf:

1. Der Client erfragt die DNS Adresse des Empfängers.

   Normalerweise würde er die IPv4 Adresse als A-Record vom DNS System zurück geliefert bekommen. Da der Client jedoch kein IPv4 mehr versteht, muss der DNS Server stattdessen einen AAAA Record an den Client senden. Dabei

IPv6 - Wenn Dual Stack nicht weiter hilft

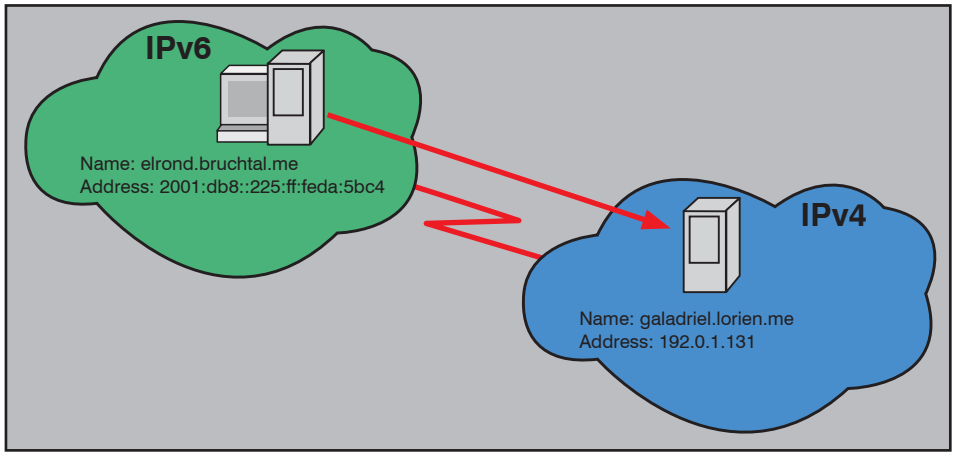


Abbildung 2: IPv6 Netzwerk mit Anbindung an einen IPv4 Provider

übersetzt er gemäß dem einem Regelwerk (s. o.: IPv4-Embedded IPv6 Adressen) die IPv4 Adresse in eine IPv6 Adresse.

2. Der Client sendet das erste Paket an den Server.

3. Auf dem Weg zum Server wird das NAT-Gateway durchlaufen.

4. Das NAT Gateway erkennt die IPv4-Embedded IPv6 Adresse und extrahiert die V4 Adresse. Diese wird im ge-NAT-eten Paket als Zieladresse eingetragen.

5. Als Quelladresse wird eine IPv4 Adresse genutzt, die sicherstellt, dass Antwortpakete des Servers zu dem NAT Gateway zurück gesendet werden.

   Außerdem wird eine NAT-Tabelle angelegt. Diese wird zum einen für weitere Pakete derselben Session genutzt und zum anderen für die Rückübersetzung benötigt.

6. Das Paket erreicht den Server im IPv4 Netz.

7. Der Server sendet das Paket zurück an das NAT Gateway.

8. Das NAT Gateway macht die Adressübersetzung anhand der NAT-Tabelle rückgängig.

9. Das Gateway sendet das Paket an den Client.

Ein Netzwerkbetreiber muss sicherstellen, dass sowohl das DNS als auch das NAT-Gateway dieselbe Methode und dieselben Parameter nutzt, um IPv4 Adressen in IPv6 Adressen ab zu bilden.

Die Punkte 5 und 8 scheinen zunächst trivial zu sein, sind es aber je nach Anwendungsfall nicht:

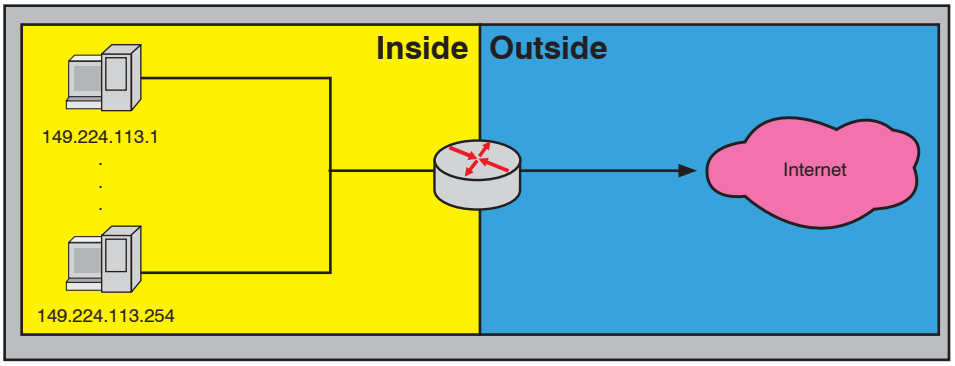
"Stateful"

Handelt es sich um eine reine Client/Server Anwendung, bei der jeglicher Verbindungsaufbau durch den Client erfolgt, so ist der Fall einfach: das NAT-Gateway wählt die IPv4 Adresse, die den Client im Internet repräsentiert, dynamisch aus einem Pool von öffentlichen IP-Adressen. Dieser Pool kann durchaus aus einer einzigen Adresse bestehen, wie das bei heimischen DSL-Routern meist der Fall ist. Das Gateway bildet ein Tubel aus Empfänger Adresse + Empfänger Port + Sender Port anhand dessen es sämtliche aktive Sessions eindeutig identifizieren kann. Das Tubel ist in Abbildung 3 in Rot dargestellt.

Der Standard für die Übersetzung zwischen IPv4 und IPv6 spricht in solch einem Fall von „Stateful", da das Gateway den Status einer Verbindung aktiv managen und beobachten muss.

„Stateless"

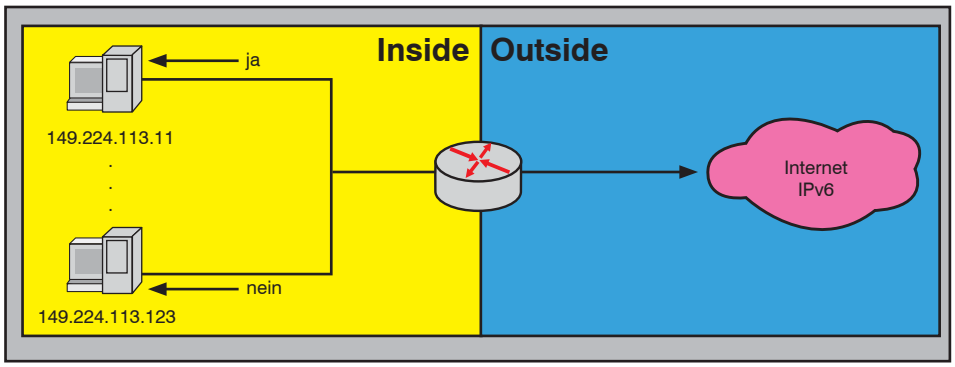
Es gibt Anwendungen, bei denen eine initiale Verbindung zwar von einem Client zunächst aufgebaut wird, jedoch in Folge dessen weitere Verbindungen benötigt werden, die von außen zum Client hin geöffnet werden. Häufig angeführte Bei-



***stateful* NAT Konfiguration**

Quell IPv4/Port	genattete Quell IPv6 Adresse/Port	Ziel IPv6 Adresse/Port
149.224.113.11/6789	2001:db8:123:456::aa:bb/6789	2001:db8:ffaa:11::aa:bb/80
149.224.113.55/1234	2001:db8:123:456::aa:bb/1234	2001:db8:ffaa:11::cc:dd/80

Abbildung 3: Beispiel einer "stateful" Konfiguration



***stateless* NAT Konfiguration**

IPv4	IPv4-Embedded IPv6 Adresse
149.224.113.11	2001:db8:123:456::149.224.113.11

Abbildung 4: Beispiel einer "stateless" Konfiguration

spiele dafür sind der Datenkanal bei aktivem FTP und über SIP aufgebaute RTP-Sessions. Um das zu ermöglichen, gibt es verschiedene Lösungsmöglichkeiten, die jedoch den Rahmen dieses Artikels sprengen würden. Als Stichwort sei hier das Application Layer Gateway (ALG) genannt.

Neben diesen Applikations-spezifischen Lösungen gibt es auch eine Lösung auf Basis von NAT, diese wird als „Stateless" bezeichnet, da das NAT Gateway zwar die Übersetzung vornimmt, das jedoch pro Paket nach einem festen Algorithmus tut, ohne irgendwelche dynamischen Tupels beim Verbindungsaufbau anlegen zu müssen.

Wie das vonstatten geht zeigt das nächste Beispiel anhand von NAT46.

NAT46

Scheint NAT64 abgesehen von der Adresseinbettung dem NAT44 sehr ähnlich zu sein, so ändert sich das, wenn man den umgekehrten Fall, NAT46, betrachtet. Wie bereits erwähnt, liegt die Schwierigkeit in diesem Falle darin, dass es erheblich mehr IPv6 als IPv4 Adressen gibt, damit gibt es keine Möglichkeit dasselbe universelle Schema wie bei NAT64 zu nutzen: IPv6-Embedded IPv4 Adressen kann es nicht für alle IPv6 Adressen geben.

Abbildung 5 zeigt eine Anwendung, die NAT46 notwendig macht: ein Unternehmen hat bereits komplett auf IPv6 umgestellt und IPv4 intern abgeschaltet. Das Unternehmen betreibt aber eigene Server, die aus dem gesamten Internet heraus erreichbar sein müssen, also auch noch von reinen IPv4 Systemen noch. Beispiele dafür sind Mail- oder Webserver.

Um das zu gewährleisten muss getrickst werden. Die einfachste Möglichkeit dafür ist die bereits erwähnte „stateless" Übersetzungsmethode. Hierbei wird im Grunde genau dasselbe gemacht wie zuvor bei NAT64 beschrieben nur umgekehrt: den eigenen Systemen werden offiziell-zugewiesene IPv4-Embedded IPv6 Adressen eindeutig zugeordnet und ins DNS eingetragen. Will nun ein externes System mit einem dieser Systeme kommunizieren, so läuft das analog zu dem in Kapitel NAT64 beschrieben Verfahren ab:

1. Das externe System erfragt die DNS Adresse des Empfängers.
   Normaler Weise würde eine IPv6 Adresse als AAAA-Record vom DNS System zurück geliefert werden. Da es sich jedoch um ein reines IPv4 System handelt, muss der DNS Server stattdessen einen A-Record an den Client senden. Dabei extrahiert er die IPv4 –Embedded Adresse aus der IPv6 Adresse.

2. Der Client sendet das erste Paket an den Server.

3. Auf dem Weg zum Server wird das NAT-Gateway durchlaufen.

4. Das NAT Gateway erkennt die IPv4 Adresse und generiert daraus die IPv4-Embedded IPv6 Adresse. Diese wird im ge-NAT-eten Paket als Zieladresse eingetragen.

5. Auch die IPv4 Quelladresse wird in eine IPv4-Embedded IPv6 Adresse umgewandelt und ersetzt.

6. Das Paket erreicht den internen Server.

7. Der Server sendet das Paket zurück.

8. Das netzinterne Routing sorgt dafür, dass das Paket zurück zum Gateway gelangt.

9. Das NAT Gateway macht die Adressübersetzung rückgängig.

10. Das Gateway sendet das Paket weiter.

An diesem Beispiel werden nun zwei Sachverhalte deutlich:

1. Anders als im ersten Beispiel ist das Anlegen einer NAT-Tabelle unnötig, da das NAT-Gateway allein anhand der Quell und Zieladressen entscheiden kann, wie die Übersetzung aussehen muss – und zwar in beide Richtungen. Deshalb: „stateless".

2. Ein weiterer Unterschied zum ersten Beispiel ist, dass das Gateway nicht seine eigene IP-Adresse in das Paket als Quelladresse einträgt, sondern eine Adresse, die sich aus einem Präfix und einer offiziellen, externen IPv4-Adresse zusammen setzt. Außerdem repräsentiert diese Adresse nie ein internes Gerät. Für genau diesen Fall bietet sich das Well-Known Präfix der IPv4-Embedded IPv6 Adressen an: im internen Netz existiert genau eine Route für das Netz 64:ff9b::/96 und diese zeigt zum NAT-Gateway.

Nachteil dieses Verfahrens ist es, dass nicht alle internen Systeme erreicht werden können, wenn man nicht ausreichend IPv4 Adressen zur Verfügung hat und das wird in den meisten Fällen der Fall sein. Damit eignet es sich zwar für ausgesuchte Serversysteme jedoch nicht für Peer-to-Peer Anwendungen wie VoIP oder für Anwendungen wie aktives FTP. Hierfür müssen dieselben oder ähnliche Mechanismen genutzt werden, wie heute bei Einsatz von NAT44 mit privaten IP Adressen.

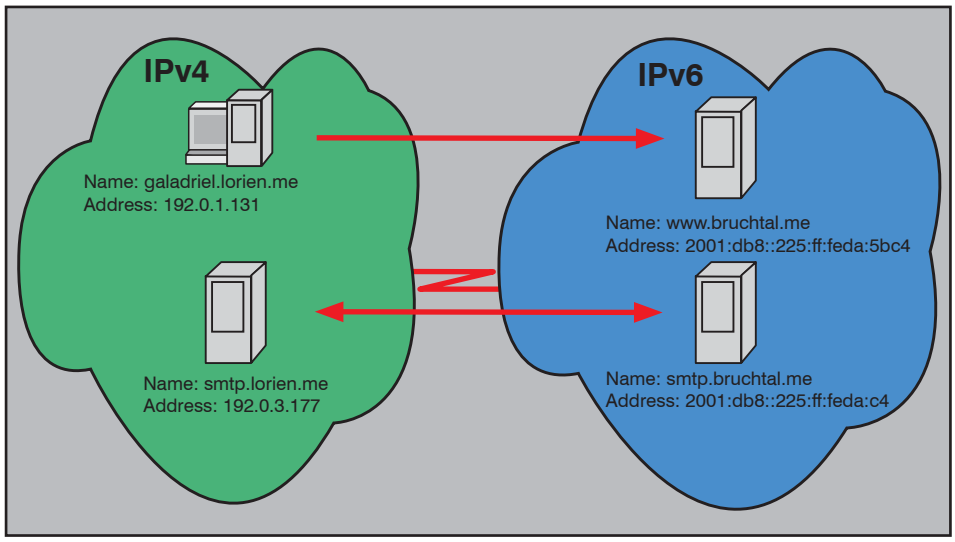


Abbildung 5: IPv4 Netzwerk mit Anbindung an einen IPv6 Provider

NAT-Konstellationen

Mittels den beschriebenen Varianten „stateless" und „stateful" lassen sich die meisten Netzwerk-Konstellationen realisieren, jedoch nicht alle. Es lohnt ein Blick auf die möglichen Varianten der Verbindungsaufbauten:

1. IPv6 Netzwerk -> IPv4 Internet
2. IPv4 Internet -> IPv6 Netzwerk
3. IPv6 Internet -> IPv4 Netzwerk
4. IPv4 Netzwerk -> IPv6 Internet
5. IPv6 Netzwerk -> IPv4 Netzwerk
6. IPv4 Netzwerk -> IPv6 Netzwerk
7. IPv6 Internet -> IPv4 Internet
8. IPv4 Internet -> IPv6 Internet

Mit „Netzwerk" sind hierbei alle Netze gemeint, die keine Providernetze (Internet) sind, vom heimischen Kleinstnetz bis hin

zu Unternehmensnetzen.

Für die Varianten 1, 2, 5 und 6 bietet stateless eine Lösung; für die Varianten 1, 3 und 5 kann (auch/alternativ) stateful zum Einsatz kommen.

Es bleiben die Varianten 4, 7 und 8. Wo ist dabei das Problem? Ganz einfach: die Anzahl genutzter IPv6 Adressen im Internet wird schnell zunehmen und damit wird es mittelfristig nicht mehr möglich sein, diese in IPv4 noch ab zu bilden. Für Variante 4 wird es wohl noch Lösungen geben, die auf den Einsatz von DNS ALGs in Kombination mit stateless NAT-Gateways beruhen, die Fälle 7 und 8 jedoch werden wegen der schieren Adressmenge für Provider nicht lösbar sein.

Was wenn auch NAT versagt?

Auf den ersten Blick scheint NAT bis auf die erwähnten drei Ausnahmen die Übergangsproblematik von reinen IPv4 in reine IPv6 Netze zu lösen. Bei genauerer Betrachtung fällt jedoch auf, dass nur die Fälle „reiner“ IPv4 bzw. „reiner“ IPv6 Netze behandelt werden und Dual Stack außen vor gelassen wird. Auch beschränkt sich der Standard auf jeweils einen einzelnen Netzübergang.

Betrachtet man das Beispiel aus Abbildung 6 sieht man, das NAT eben nicht alle Probleme löst. Dabei ist der dargestellte Fall nicht aus der Luft gegriffen, sondern beruht im Gegenteil auf den Erfahrungen des Autors.

Die wichtigsten Fakten zur Ausgangslage:

- Der Anschluss an ein IPv6 Providerbackbone ist noch nicht realisiert, wird jedoch bald erfolgen.
- Das interne Unternehmensnetz wurde bereits auf Dual-Stack umgestellt.
- Die Anschaffung einer IPv6 fähigen Firewall, die auch das Default Gateway der Clients ist, soll erst kurz vor der Anschaltung an das Provider Netz erfolgen.
- Die IPv6 Aufgaben übernimmt bis zur Anschaffung der Firewall ein Microsoft 2008 Server, auf dem auch DHCPv6 aktiviert ist.
- Es werden eigene DNS-Server von Microsoft betrieben.
- Auf den Clients kommen während des Pilotprojektes die Betriebssysteme Windows 7 und Mac OS X zum Einsatz.

Was die beteiligten Microsoft Clients an-

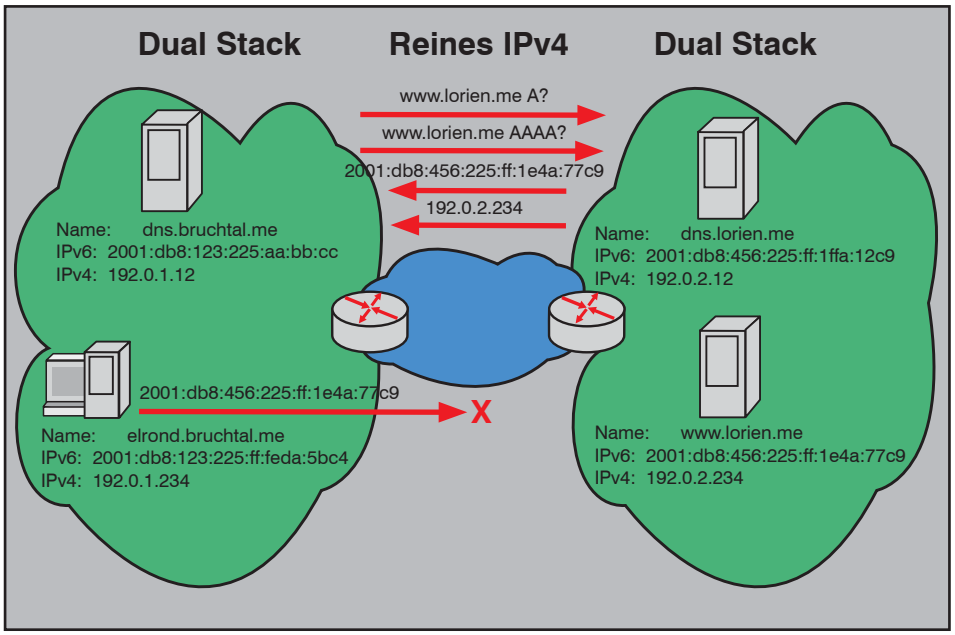


Abbildung 6: Dual Stack Problem bei Providern ohne NAT

geht, so funktioniert – bislang – auch alles problemlos. Bei dem einzelnen Mac OS X Client sieht das jedoch anders aus: die interne Kommunikation funktioniert auch bei dem Apple einwandfrei und auf die meisten Ressourcen im Internet kann ebenfalls ohne Probleme zugegriffen werden. Allerdings gibt es einige Webseiten, die nur sehr langsam aufgebaut werden. Schaltet man IPv6 auf dem Mac aus, so werden dieselben Webseiten sehr zügig angezeigt.

Eine Analyse brachte folgende Erkenntnisse:

1. Nur Webseiten, die neben einer IPv4 auch eine IPv6 Adresse haben, sind betroffen.
2. Die Windows 7 Clients tragen kein Default Gateway für IPv6 ein.
3. Der Mac Client trägt die Link Local IPv6 Adresse des Microsoft Servers als Default Gateway ein.

Abbildung 7 zeigt das typische Verhalten heutiger Browser in solch einem Fall: zunächst wird versucht, das bevorzugte IPv6 Protokoll zu benutzen, dazu wird ein TCP SYN über IPv6 an den Server geschickt. Das Paket wird jedoch niemals bei dem Webserver ankommen, da es von dem ISP nicht weitergeleitet werden kann. Im günstigsten Fall bekommt der Client ein ICMP „Protcol unreachable“, leitet die Information an den Browser und dieser behält sich die Information für die weitere Kommunikation mit diesem Server. Das ist im Beispiel jedoch nicht der Fall. Der Browser wird somit auf den Ablauf eines Timers warten, der typischerweise mehrere Sekunden beträgt, und den Vorgang noch 2x wiederholen. Erst danach versucht er es mit IPv4. Übrigens versucht es der Mac nicht nur für den Aufruf der ersten Seite, sondern für jede einzelne TCP-Verbindung erneut zunächst mit IPv6.

Was der User dabei erlebt, wird sich ihm unweigerlich für die kommenden Jahre ins Gehirn einbrennen: IPv6 ist langsam.

Natürlich kann man nun sagen, dass es sich hier um einen Spezialfall handelt und entweder Microsoft oder Apple Abhilfe schaffen müssten und dass diese Situation nur entsteht, wenn man nicht mit einem „ordentlichen“ IPv6 Router arbeitet. Aber zum einen wird diese Konstellation wohl des Öfteren in IPv6 Pilotprojekten vorkommen, zum anderen kann es auch andere Situationen geben, die zu demselben Effekt führen und zwar dann, wenn zwischen Sender und Empfänger mehrere ISPs liegen, die unterschiedliche Stadien der Migration erreicht haben.

Aktion: Glückliche Augen

Auch die IETF hat dieses Problem erkannt und arbeitet an einer Lösung, die unter dem Namen „Happy Eyeballs: Trending Towards Success with Dual-Stack Hosts“ läuft. Der Draft hat zwar noch die Nummer 1, jedoch ist er ein direkter Nachfahre eines anderen und erweitert diesen, indem er die Beschränkung auf Browser als Anwendung aufhebt. Ziel ist es dabei nicht nur, sicher zu stellen, das eine Verbindung zustande kommt, sondern dass im Zweifelsfall die performanteste Verbindung gewählt wird, selbst wenn beide IP Protokoll-

IPv6 - Wenn Dual Stack nicht weiter hilft

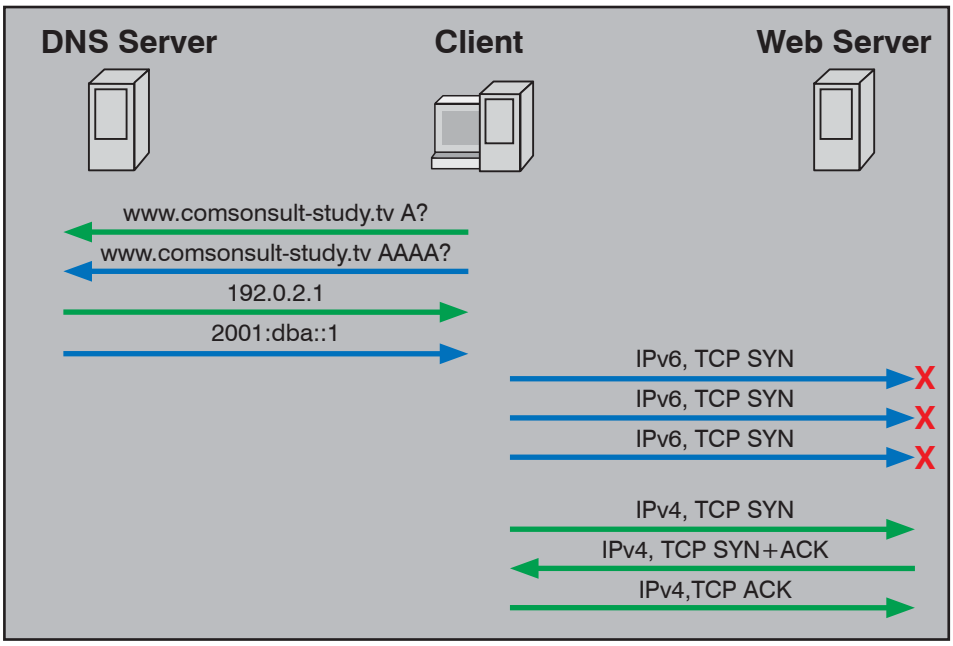


Abbildung 7: Browserverhalten bei nicht durchgehender IPv6 Verbindung

versionen zur Verfügung stehen.

Der Vorschlag basiert auf einer Anpassung der „zeitsensitiven", Dual Stack fähigen Applikationen. Bei diesen wird ein Parameter P eingeführt, über den geregelt wird, welches Protokoll für welche Verbindung bevorzugt genutzt werden soll. Dabei soll jede Applikation für jedes Ziel einen eigenen Parameter pflegen. Ist P negativ, so wird IPv4 bevorzugt, ist P positiv IPv6.

Für das bevorzugte Protokoll läuft der Verbindungsversuch wie gewohnt ab. Für das andere Protokoll wird die DNS Anfrage um P*10 Millisekunden verzögert. Im Falle von IPv4 (negativer Wert für P) wird das Vorzeichen ignoriert. Hat die Anwendung nach Ablauf der Verzögerung noch keine Antwort erhalten, so wird versucht auch für das weniger präferierte Protokoll eine Verbindung aufzubauen.

Sobald eine Verbindung zu Stande gekommen ist, wird der Wert für P angepasst. Dabei gibt es zwei Möglichkeiten:

1. Ist das präferierte Protokoll schneller, wird der absolute Wert von P um eins erhöht, vgl. Abbildung 8 (Beispiel: aus 4 wird 5 und aus -4 wird -5).

2. Ist das andere Protokoll schneller, so wird der Wert von P halbiert und gegebenenfalls abgerundet, vgl. Abbildung 9 (Beispiele: aus 9 wird 4 und aus 1 wird 0).

Sofern sie überhaupt aufgebaut wurde, so soll die langsamere Verbindung anschließend abgebaut werden. Der Grenzwert für P soll 400 sein, was einer DNS Verzögerung von 4 Sekunden entspricht.

Dieses Verfahren funktioniert natürlich, hat aber Nachteile:

- Der Client wird so lange für jede IP Version TCP Sitzungen zu einem Zielsystem starten, bis der Wert für P groß genug geworden ist, dass die Verzögerung ausreicht, um vom Server eine Antwort zu erhalten.

  Denkt man dabei an Web-Browsing, so werden oft sehr viele TCP Sitzungen in sehr schneller Abfolge geöffnet und es dürften eine Menge Erhöhungen um 10 Millisekunden erforderlich sein, bis bei einer transkontinentalen Verbindung die Verzögerung groß genug geworden ist.

  In Folge dessen werden erheblich mehr TCP Verbindungsanfragen an die Webserver gestellt, als notwendig wären, was zu einer erheblichen Mehrbelastung der Server führt. Viele Webserver haben Limits für Anzahl von TCP-Sessions, um sich vor Überlastungen zu schützen.

- Es steht zu befürchten, dass für lange Zeit IPv4 schneller bearbeitet wird als IPv6. Beispielsweise transportieren nicht alle Netzwerkkomponenten IPv6 eben so schnell wie IPv4.

  Infolge dessen wird IPv4 gegenüber IPv6 bevorzugt und das, obwohl das eigentlich erklärte Ziel ist, IPv4 abzuschaffen. So lange aber (scheinbar) IPv4 präferiert wird, werden gerade Entwickler von zeitkritischen Anwendungen darauf den Fokus legen.

- Das Verfahren ist nur für TCP spezifiziert und ignoriert somit automatisch ausgerechnet zeitkritische RTP-basierte Dienste wie VoIP und Video.

- Das Verfahren muss in die Applikationen integriert werden und nicht in den Dual Stack. Man kann also davon ausgehen, dass es Anwendungen geben wird, die das Verfahren unterstützen und (deutlich mehr) Anwendungen, die das nicht tun werden.

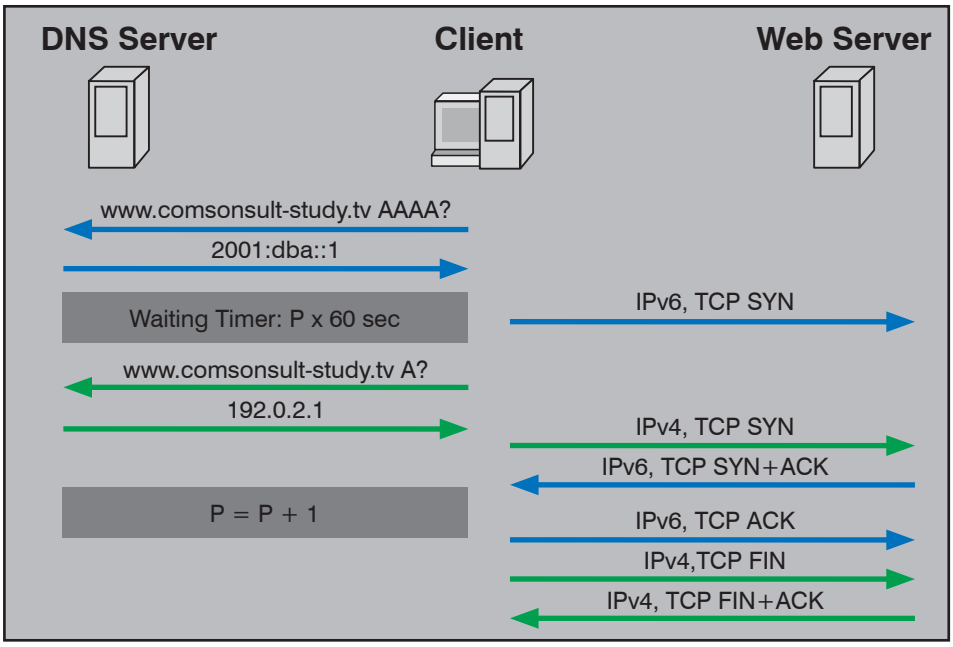


Abbildung 8: Verbindungsaufbau mit "Happy Eyeballs", wenn beide Protokolle funktionieren und das bevorzugte Protokoll schneller ist

IPv6 - Wenn Dual Stack nicht weiter hilft

Parallele Welten

Schon das Wort „Migration“ legt nahe, dass der Übergang von IPv4 auf IPv6 keine Nacht- und Nebelaktion werden wird, in der von heute auf morgen das Protokoll ausgetauscht werden kann. Für einen wohl recht langen Zeitraum werden beide Protokolle parallel betrieben werden müssen. Zwar teilen sich beide Protokolle denselben Namen (Internet Protokoll), dieselbe Abkürzung (IP), dieselbe OSI-Schicht (3) und dieselben Nachbarn (Protokolle der Schichten 2 und 4), was die Interoperabilität angeht, so hört damit aber die Harmonie auch schon auf. Auf Schicht 3 haben beide Protokolle so viel gemeinsam wie IPX mit AppleTalk: man versteht sich nicht. Anders als bei IPX und AppleTalk handelt es sich jedoch nicht um Parallelentwicklungen, sondern beide stammen aus demselben Haus, so dass es immerhin möglich ist, die Kompatibilität bei der Entwicklung mit einzubeziehen.

Die beiden vorgestellten Verfahren gehören in diese Gruppe von Kompatibiltätsmechanismen. Und beide zeigen deutlich, dass es sich dabei nur um Übergangstechnologien handeln kann, da sie entweder, wie bei NAT, nicht alle Fälle abdecken können, oder, wie bei den Happy Eyeballs, nicht alle Applikationen unterstützten.

Ferner fällt auf, dass beide Standards sehr jungen Datums sind, so als wären die Entwickler von IPv6 davon überrascht worden. Das wiederum zeigt, dass IPv6 noch nicht vollständig „ausgewachsen“ ist. Womit das Fazit nur heißen kann: die kommenden Jahre werden spannend.

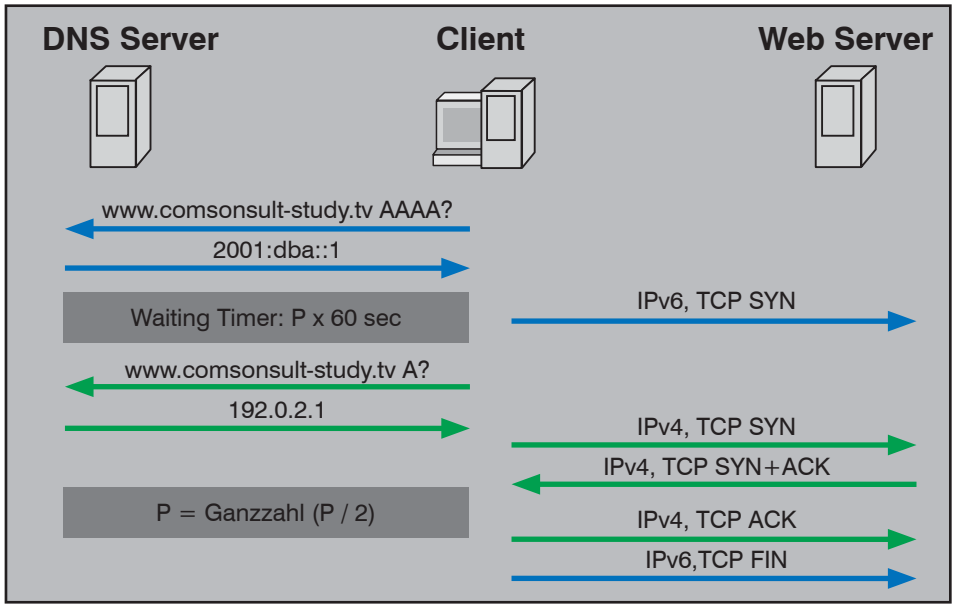


Abbildung 9: Verbindungsaufbau mit "Happy Eyeballs", wenn entweder das niedriger priorisierte Protokoll schneller antwortet oder das höher priorisierte keine Ende-zu-Ende Verbindung aufbauen kann

Anhang

Abkürzungsverzeichnis

ALG	Application Layer Gateway
DHCP	Dynamic Host Configuration Protocol
DNS	Dynamic Name Service
DSL	Digital Subscriber Line
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IPX	Internetwork Packet eXchange
ISP	Internet Service Provider
NAT	Network Address Translation
OSI	Open Systems Interconnection
RFC	Request for Comments
RTP	Real Time Protocol
SMTP	Simple Mail Transport Protocol
TCP	Transmission Control Protocol
VoIP	Voice over IP

Literaturverzeichnis

- Dipl.-Inform. Petra Borowka-Gatzweiler, „IP Version 6 - Das Internet der nächsten Generation (Teil 2)“, Netzwerk Insider April 2010
- Dipl.-Inform. Dietlind Hübner, Dipl.-Inform. Oliver Flüs , „Einstieg in IPv6 – (nicht nur) am Beispiel Adressplanung und ‚Direct Access‘“, Netzwerk Insider Januar 2011
- C. Bao, C. Huitema, M. Bagnulo, M. Boucadair, X. Li, "IPv6 Addressing of IPv4/IPv6 Translators", RFC 6052
- Fred Baker, Xing Li, Congxiao Bao, Kevin Yin, "Framework for IPv4/IPv6 Translation", draft-ietf-behave-v6v4-framework-10
- M. Bagnulo, A. Sullivan, P. Matthews, I. van Beijnum, „DNS64: DNS extensions for Network Address Translation from IPv6 Clients to IPv4 Servers“, draft-ietf-behave-dns64-11
- X. Li, C. Bao, F. Baker, "IP/ICMP Translation Algorithm", draft-ietf-behave-v6v4-xlate-23
- M. Bagnulo, P. Matthews, I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", draft-ietf-behave-v6v4-xlate-stateful-12
- D. Wing, A. Yourtchenko, "Happy Eyeballs: Trending Towards Success with Dual-Stack Hosts", draft-wing-v6ops-happy-eyeballs-ipv6-01
- D. Wing, A. Yourtchenko, P. Natarajan, Happy Eyeballs: Trending Towards Success (IPv6 and SCTP), draft-wing-http-new-tech-01

Kongress

ComConsult IPv6-Forum 2011
09.05. - 11.05.11 in Königswinter

Der Wechsel von IPv4 auf IPv6 ist unvermeidbar und wird in 2011 weltweit im großen Stil beginnen. Dabei liefert IPv6 nicht nur einen neuen Adressraum sondern ein völlig verändertes Betriebsszenario. DNS, DHCP und wesentliche Teile der vorhandenen Sicherheits-Lösungen müssen neu durchdacht und angepasst werden. Speziell Firewall- und NAT-Installationen sind betroffen.

Moderation: Markus Schaub
Preis: € 1.990,-- zzgl. MwSt.

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

Standpunkt Sicherheit

Herausforderung Data Loss Prevention

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.

Die grundlegende Anforderung für ein System zur Data Loss Prevention (auch als Data Leakage Prevention bezeichnet, kurz: DLP) ist erschreckend einfach gestellt („es ist zu verhindern, dass entsprechend klassifizierte Daten einen wohl definierten Bereich verlassen“) jedoch nur ausgesprochen schwer umsetzbar.

Die Basis ist die Klassifizierung der Daten: Welche Daten dürfen das Unternehmen ohne Einschränkung verlassen, welche Daten müssen intern und welche (ggf. sogar streng) vertraulich bleiben. Auch wenn man sich z.B. in militärischen Bereichen daran gewöhnt hat: Eine solche Klassifikation ist nicht trivial. Aus dem Blickwinkel der Daten ist es zwar nur ein einfaches Attribut, das die Vertraulichkeit festlegt, die Frage ist jedoch, wer legt dies fest und nach welchen Kriterien. Ohne klare Richtlinien, die allgemein bekannt sind und routiniert umgesetzt werden, geht es nicht. Klassifikationen werden objektweise (z.B. pro Datei bzw. Dokument) oder gruppenweise gemacht. Auch dies sagt sich leicht. Wer übernimmt die Fleißarbeit für den Bestand an nicht klassifizierten Daten?

Für klassifizierte Daten müssen Berechtigungen festgelegt werden, d.h. insbesondere wer die Daten wo einsehen darf bzw. in welchen Bereichen sich klassifizierte Daten bewegen dürfen. Diese Bereiche können organisatorisch durch eine Gruppenzugehörigkeit, räumlich, durch einen Verbund von IT-Komponenten oder eine Kombination hieraus festgelegt sein. Wenn Daten zwar ordnungsgemäß klassifiziert werden, jedoch der Kreis der Personen, die Zugriff auf vertrauliche Daten haben, nicht strikt auf das notwendige Minimum reduziert wird und die Berechtigungen keinem Kontrollprozess unterliegen, braucht man sich trotzdem nicht über einen Datenabfluss zu wundern. WikiLeaks hat es vorgemacht: Für die USA ist es so zu einem diplomatischen GAU gekommen, als eine Vielzahl von ausgesprochen vertraulichen Dokumenten (die selbstverständlich gesichert übertragen, aufbewahrt sowie ordnungsgemäß klassifiziert wurden) in Richtung WikiLeaks abgeflossen sind.

Dokumente auf mobilen Datenträgern, in E-Mail Attachments, auf Servern zum Datenaustausch, die das Unternehmen nicht hätten verlassen dürfen, waren zunächst die klassischen Bereiche, auf die DLP-Lösungen sich konzentriert haben. Später hinzugekommen sind Mobiltelefone, Smartphones und Tablets als Quelle eines Verlusts von Daten. Außerdem sind mit Instant Messaging, Unified Communications, Kollaborationsplattformen und schließlich Cloud Computing neue Wege für den unerwünschten Abfluss kritischer Daten zu berücksichtigen.

Letztendlich müssen alle Schnittstellen, über die Daten den für sie vorgesehen Bereich verlassen könnten, durch entsprechende Werkzeuge überwacht werden. Dies erfordert zunächst Agenten auf allen relevanten Endsystemen (Clients und Servern), welche Daten verschlüsseln, den Nutzer auf Verletzungen von Policies hinweisen und ggf. Aktionen blockieren. Außerdem ist ein übergreifendes Schlüssel- und Identitätsmanagement notwendig, damit nur die berechtigten Nutzer Zugriff auf die Daten bekommen. Ergänzend kommen für Überwachungsaufgaben auch Security-Gateways (z.B. zur Absicherung von Web-Zugriffen und E-Mail) in Frage.

Damit eine DLP-Lösung das verlangte leistet, müssen insgesamt neben dem entsprechenden Werkzeugeinsatz die Konzepte für Dokumentenverwaltung, Identitätsmanagement, Berechtigungskontrolle, Verschlüsselung, Zugangs- und Zugriffskontrolle und Überwachung um DLP-Aspekte ergänzt werden. Diese Wirkkette, die verschiedenste Bereiche der Informationstechnik umspannt, kann nur in einer durchgehend prozessgesteuerten Informationstechnik funktionieren, also einer Prozesslandschaft, die auch tatsächlich in der Organisation konsequent gelebt wird. Genauso wichtig ist die nachhaltige Sensibilisierung der Nutzer, denn DLP-Lösungen können Risiken durch Nachlässigkeit nicht vollständig ausschließen.

DLP ist als eine Kerndisziplin der Informationssicherheit zu sehen, und trotz der Komplexität muss man sich der Herausforderung DLP stellen. Hier geht es nicht nur um Spionage, auch ein Reputationsschaden kann immense Auswirkungen haben.

Kongress

IT-Sicherheits-Forum 2011
23.05. - 24.05.11 in Königswinter

Das IT-Sicherheits-Forum wird auch im Jahr 2011 wieder einen umfassenden Überblick zu aktuellen Themen der IT-Sicherheit in Theorie und Praxis anbieten. Dabei wird äußerst hoher Wert auf sofort verwendbare Informationen gelegt, die Teilnehmer sollen die gewonnenen Erkenntnisse möglichst sofort in der eigenen Umgebung anwenden können.

Moderation: Dr. Simon Hoff
Preis: € 1.790,-- zzgl. MwSt.

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

Aktuelles Seminar

E-Mail-Archivierung planen, evaluieren, umsetzen

Die ComConsult Akademie veranstaltet vom 16.05. - 18.05.11 ihr Seminar „E-Mail-Archivierung planen, evaluieren, umsetzen“ in Bonn.

Das Seminar „E-Mail-Archivierung planen, evaluieren, umsetzen“ richtet sich insbesondere auch an Teilnehmer aus dem Bereich des öffentlichen Dienstes, der ebenso wie private Unternehmen zur Aufbewahrung von E-Mails verpflichtet ist. Es gibt wenige Seminare zur E-Mail-Archivierung, in denen die besonderen Aspekte zu den Aufbewahrungspflichten und die abweichenden Bestimmungen der Landesdatenschutzgesetze thematisiert werden.

Obwohl die allgemeinen Aufbewahrungsvorschriften aus dem Handelsgesetzbuch und dem Steuerrecht nicht direkt anwendbar sind, gibt es zahlreiche Vorschriften zur Aufbewahrung im öffentlichen Dienst, die nicht so leicht erkennbar sind wie im nichtöffentlichen Bereich. Dazu gehören u.a. Verwaltungsvorschriften, Haushaltsgesetze, Gesetzbindungs- und Beweisregeln sowie Archivgesetze. Das Haushaltsgrundsätzegesetz des Bundes von 2009 und die bevorstehende Einführung der Doppik in der Verwaltung erzwingen eine analoge Anwendung des § 257 HGB. Im Seminar werden auch die Besonderheiten der Landesdatenschutzgesetze im Vergleich zu den Regeln des Bundesdatenschutzgesetzes für Unternehmen behandelt.

In diesem Seminar lernen Sie

- welche Daten nach gesetzlichen Vorgaben gespeichert werden müssen
- welche Daten aus eigenem Interesse gespeichert werden sollten
- welche Haftungsrisiken in zivil- und strafrechtlicher Hinsicht bei Missachtung der Vorschriften drohen
- welche Zugriffs- und Überwachungsmöglichkeiten staatlichen Stellen zustehen
- wie lange die Aufbewahrungsfristen für einzelne Datenkategorien sind
- wie die Rechtslage in anderen EU-Ländern, in der Schweiz und den USA dazu aussieht
- in welchen Formaten Daten zu archivieren sind
- wie mit verschlüsselten Daten umzugehen ist
- wie ein Archivierungsprojekt aufgebaut werden sollten welche organisatorischen Voraussetzungen vor dem Beginn eines Archivierungsprojektes geschaffen werden sollten
- welche Aspekte bei der Evaluierung von Produkten berücksichtigt werden müssen
- welche Schnittstellen zu anderen Softwareprodukten geschaffen werden müssen

Referenten dieses Seminars

Ulrich Emmert ist Rechtsanwalt in der Kanzlei esb Rechtsanwälte. Ein Schwerpunkt seiner Tätigkeit sind Beratungen und Schulungen im Bereich des EDV-, Telekommunikations– und Online-Rechts. Dabei kommen ihm umfangreiche technische Kenntnisse im Bereich Programmierung, Datenbanken und Internet-Security (Digitale Signaturen, Firewalls) zugute, die auch eine qualifizierte Beratung im Bereich Netzwerksicherheit, Softwarelizenzverträge oder Datenschutz ermöglichen.

Daniel Maiworm ist Berater bei GlassHouse Technologies mit den Schwerpunkten Elektronische Archivierung, e-Discovery und Data-Loss-Prevention (DLP). Seit 2001 betreut er E-Mail Archivprojekte für internationale Konzerne und bekannte öffentliche Einrichtungen. In einer Fallstudie präsentiert er die typischen Schwierigkeiten eines Archivprojekts, diskutiert die möglichen Handlungsoptionen und zeigt pragmatische Lösungsansätze auf.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

E-Mail-Archivierung planen, evaluieren, umsetzen

Ich buche das Seminar
E-Mail-Archivierung planen, evaluieren, umsetzen

☐ **16.05. - 18.05.11 in Bonn**
☐ **07.11. - 09.11.11 in Königswinter**

zum Preis von € 1.890,-- zzgl. MwSt.

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

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

Schwerpunkthema

Cloud Storage: wer braucht das überhaupt?

Fortsetzung von Seite 1

Dr. Behrooz Moayeri ist in der ComConsult Beratung und Planung GmbH als Mitglied der Geschäftsleitung tätig. Er hat in den letzten Jahren unter anderem viele Unternehmen im Storage-Bereich beraten.

Hinzu kommen die Unannehmlichkeiten des Wechsels, wenn mal wieder die zentralisierten Speichersysteme an ihre Kapazitäts- und Skalierbarkeitsgrenzen stoßen. Und das passiert in immer kürzeren Abständen. Leidgeprüft müssen die IT-Abteilungen alle drei bis vier Jahre größere Storage-Renovierungsprojekte einplanen. Und wer kennt die Strapazen eines solchen Projektes nicht: Risiken bei der Umstellung, genervte Anwender, Nacht- und Wochenendarbeit, unzufriedene Manager, die eine reibungslosere Umstellung erwartet hatten.

Das Terrain ist bereit für ein Allheilversprechen: Cloud Storage. Warum mühselig eigene Speicherstrukturen aufbauen, wenn man Speicherplatz extern kaufen kann? Betreibe ich ein Kraftwerk, wenn ich Strom brauche? Also weg mit dem Ärger! Um die Abdeckung meines Speicherbedarfs sollen sich die kümmern, die das nicht nur für mich machen müssen. Die Storage Coud Provider haben offenbar den dynamischen Wachstumsprozess im Griff. Auch wenn sie Systeme hinzufügen oder ersetzen, merken die Kunden nichts davon. Alles läuft wie geschmiert: Migrationen, Erweiterungen, Verlagerungen etc.

Bei einem solchen Heilversprechen ist die Verlockung groß, auf Cloud Storage zu setzen. Man braucht weniger Personal, bezahlt nur so viel Speicher wie man braucht, hat keine Umstellungsrisiken. Alles wird gut.

Wir wollen mit diesem Beitrag das Gegenteil beweisen, nämlich dass Cloud Storage für die meisten mittleren bis großen Unternehmen nicht funktionieren wird.

Begriffsklärung

Zunächst ist eine Begriffsklärung notwendig: Was ist Cloud Storage? Hier ist zu differenzieren zwischen:

- dem Basisdienst, bei dem der Provider nur Speicherplatz zur Verfügung stellt (dargestellt in der Abbildung 1), und
- dem erweiterten Dienst, der über den Basisdienst hinaus auch ein Hosting der Applikation durch den Provider vorsieht (dargestellt in der Abbildung 2).

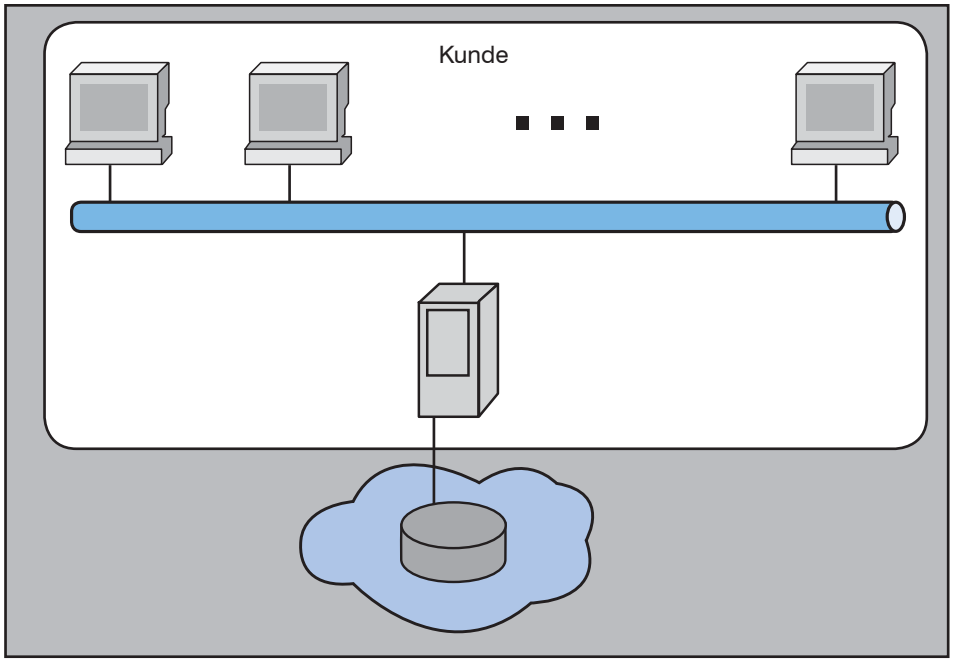


Abbildung 1: Basisdienst Cloud Storage

Wenn im Folgenden von Cloud Storage gesprochen wird, ist in erster Linie der Basisdienst gemeint.

Ferner ist Cloud Storage abzugrenzen vom Betrieb dedizierter Speichersysteme für ein Unternehmen durch einen Provider, manchmal als „Storage on Demand“ bezeichnet. Dieser Dienst ist älter als Cloud Storage und wird zum Beispiel dann in Anspruch genommen, wenn ein Unternehmen ein gewisses Maß an Planungssicherheit durch vertraglich festgelegte Kosten pro Gigabyte erlangen und nicht durch einen sprunghaften Anstieg der Speicherkosten aufgrund eines Investitionszyklus belastet werden will.

Wo sind die wirklichen Probleme?

Um zu prüfen, ob Cloud Storage das mit diesem Dienst verbundene Heilversprechen hält, müssen wir uns die wirklichen Probleme anschauen, die mit den heutigen Speicherstrukturen verbunden sind. Wodurch werden die Kosten verursacht? Welche sind die Risiken? Was bereitet den Speicherverantwortlichen schlaflose Nächte?

Cloud Storage: wer braucht das überhaupt?

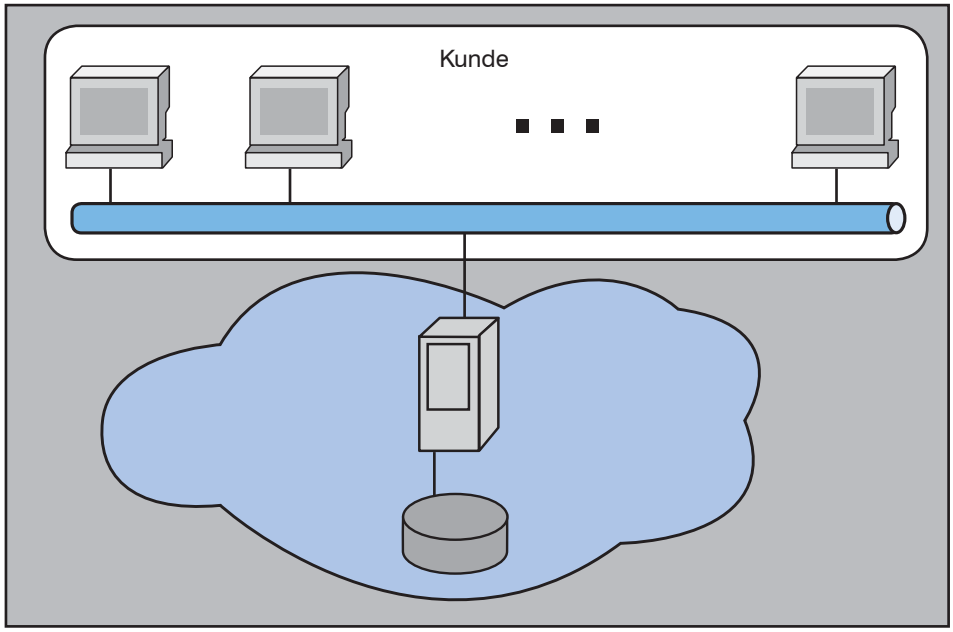


Abbildung 2: Erweiterter Dienst einschließlich Applikation und Storage

Wir werden das Beispiel eines fiktiven Unternehmens unter die Lupe nehmen. Ähnlichkeiten mit real existierenden Unternehmen sind rein zufällig (oder vielleicht auch nicht).

Die IT-Landschaft des Beispielunternehmens ist in der Abbildung 3 dargestellt. Verschiedene Standorte des Unternehmens sind über das Wide Area Network (WAN) mit dem Rechenzentrum verbunden, das zwar auf zwei Standorte verteilt, aber abstrakt als ein zusammenhängender Bereich dargestellt ist. Die physikalische Netzstruktur des Rechenzentrums, bestehend aus einem Local Area Network (LAN) und einem Storage Area Network (SAN), ist in der Abbildung 3 ausgeblendet. Zunächst interessiert uns nur die Applikationslandschaft.

Diese ist historisch gewachsen und enthält unter anderem Server für folgende Anwendungen:

- E-Mail
- Unified Communications
- Contact Center
- Datenbanken
- Web
- E-Business
- Computer-Telefonie-Integration (CTI)
- Customer Relationship Management (CRM)

In der Abbildung 3 sind Server-Server-Kommunikationsbeziehungen dargestellt. Entweder in den Applikationen selbst oder als Batch Jobs organisiert werden laufend Daten zwischen den Servern ausgetauscht. Es bestehen Wechselbeziehungen zwischen verschiedenen Datenbanken. Jede Datenbank unterhält vielfältige Import- und Exportbeziehungen zu anderen Datenbanken.

Wenn in einer solchen Umgebung Speicherressourcen zentralisiert sind und von verschiedenen Applikationen geteilt werden, heißt es noch lange nicht, dass die Speichersysteme den Datenaustausch zwischen den Anwendungen autark organisieren. Der zentralisierte Speicher ist in unterschiedliche logische Einheiten (Logical Units, LUNs) eingeteilt, die den Servern eindeutig zugeordnet sind. Die Daten jeder LUN unterliegen der Hoheit einer Datenbank- oder Applikationsinstanz. Nur über diese Instanz wird auf diese Daten lesend oder schreibend zugegriffen. Daher ist der Datenaustausch zwischen Anwendungen vor allem Austausch zwischen verschiedenen Serverinstanzen. Wenn Daten von der Datenbank A in die Datenbank B exportiert werden, werden sie vom Datenbankserver A aus dem SAN ausgelesen, über das LAN zum Daten-

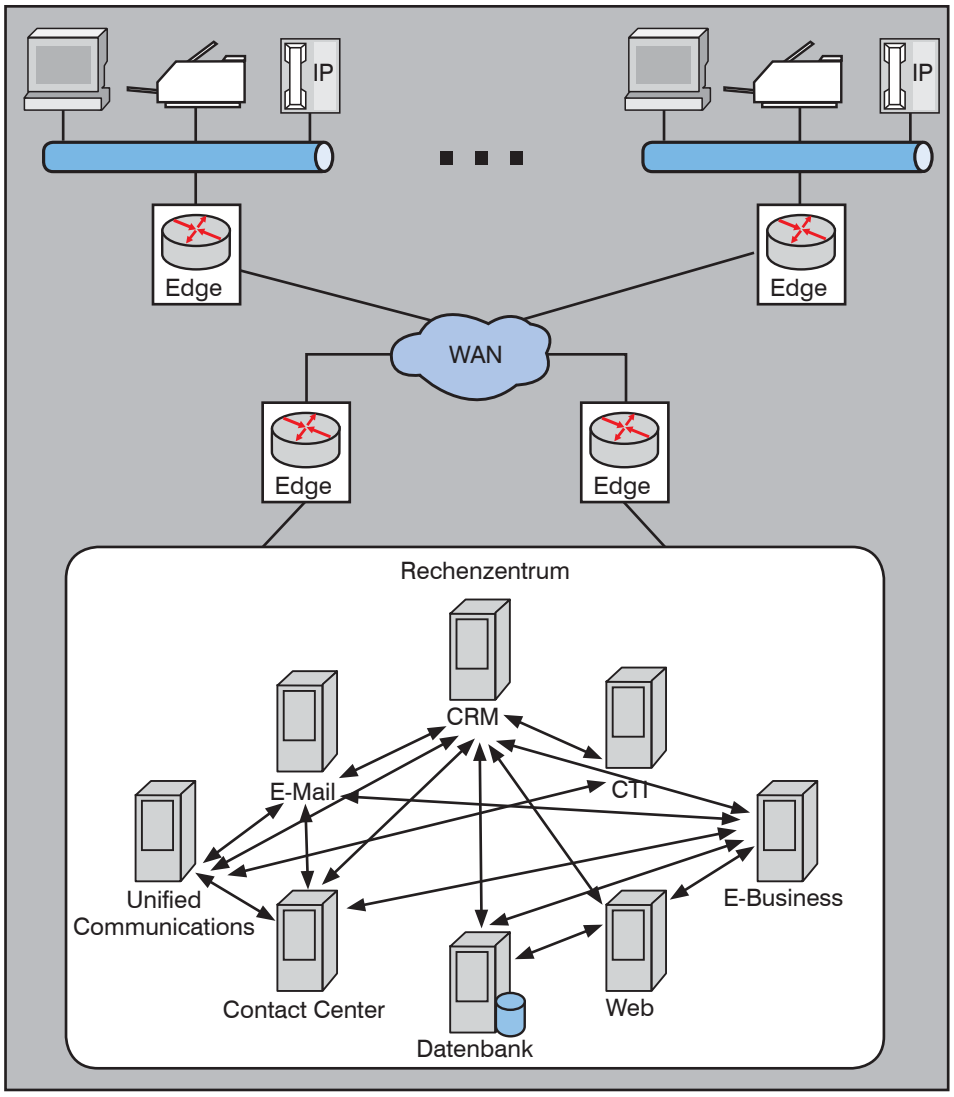


Abbildung 3: IT-Landschaft eine Beispielunternehmens

bankserver B transferiert, dort möglicherweise verarbeitet und wieder in das SAN geschrieben.

Nun stelle man sich vor, für diese Systemlandschaft soll ein Datensicherungskonzept ausgearbeitet und umgesetzt werden. Ziel ist eine zentrale Datensicherung, mit einer Hierarchie von Speichermedien, von Disc-to-Disc Storage über Virtual Tape Library (VTL) bis zu einem Bandroboter bzw. einem Archivierungssystem mit optischen Medien.

Auf dem Backupserver werden Sicherungsjobs definiert, die der Server teilweise parallel, teilweise sequentiell abarbeitet.

Nun kommt es dazu, dass eine der Datenbanken ein Problem aufweist. Ursachen für solche Probleme können vielfältig sein:

- Hardware-Ausfall: Die Wahrscheinlichkeit solcher Probleme kann durch die redundante Gestaltung von Servern, Netz und Speicher minimiert werden.
- RZ-Ausfall: Ein kompletter Standort kann ausfallen, sei es durch Stromausfall, Hochwasser, Brand, Ausfall der Klimaanlage, Erdbeben, Tsunami etc. Von einem solchen Szenario ist jedoch in den meisten Fällen nur ein Standort betroffen, wenn der zweite Standort in einer ausreichenden Entfernung vom ersten liegt. Für solche Katastrophenfälle kann durch die ausfallsichere Verteilung von Servern und Speichersystemen auf die RZ-Standorte vorgesorgt werden.

- Software-Problem: Auf einem der Server führt ein Software-Bug dazu, dass korrumpierte Daten in eine Datenbank geschrieben werden. Das Problem kann sich durch die Import- und Exportbeziehungen zwischen den Datenbanken binnen kurzer Zeit fortpflanzen und auch andere Datenbanken betreffen.

- Arbeitsfehler: Einem Administrator unterläuft ein Fehler, bei dem eine Datenbank unbeabsichtigt verändert wird. Auch bei diesem Szenario kann sich das Problem auf andere Datenbanken fortpflanzen.

Die Datensicherung soll Vorkehrungen gegen alle diese Szenarien beinhalten. Dabei tritt das letztgenannte Szenario, in dem das Problem auf menschliches Versagen zurückzuführen ist, wesentlich häufiger ein als zum Beispiel ein RZ-Ausfall. Hardware kann zwar ausfallen, aber eine dem Stand der Technik entsprechende IT-Landschaft weist eine Reihe von Sicherheiten gegen Auswirkungen von Hardware-Ausfällen auf, von Redundant Array of Independent Disks (RAID) in den Speichersystemen bis hin zu gespiegelten Storage Arrays.

Diese Vorkehrungen sind aber bei einem menschlichen Versagen oder einem Software-Problem unwirksam. Insbesondere für solche Szenarien ist die Wiederherstellung von gesicherten Daten gedacht. Die Daten sollen auf einen Stand zurückgeführt werden können, bei dem das Problem noch nicht eingetreten war.

Nun kommen wir auf die Vielfalt der Beziehungen zwischen den Systemen zurück: Wann war der Zeitpunkt, zu dem ein konsistenter Stand aller Datenbanken existierte? Wie lässt sich dieser Zeitpunkt finden? Ein Ziel ist natürlich, intakte Datenbanken nicht unnötig auf frühere Stände zurückzuführen, denn je weiter diese Stände in der Vergangenheit liegen, desto größer ist der Daten- und der Produktivitätsverlust. Man stelle sich vor (siehe Abbildung 4):

- Die Datenbank A wurde um 14:52 Uhr korrumpiert.

- Das Problem wurde um 16:13 Uhr bemerkt.

- Um 15 Uhr erfolgte ein Export aus der Datenbank A in die Datenbanken C und F.

- Um 16 Uhr pflanzte sich das Problem auf die Datenbanken B, D und E fort.

Für die Reparatur der Datenbanken werden nicht nur eine funktionierende Datensicherung, sondern auch detaillierte Kenntnisse der Wechselbeziehungen zwischen den Datenbanken benötigt. Um gezielt die Datensicherungsbestände zu identifizieren, welche ein Minimum an Datenverlust und dennoch einen konsistenten, unkorrumpierten Gesamtbestand der Datenbanken wiederherstellen können, greift man in der Praxis nicht nur auf die Sicherungsmedien zu, sondern auf Archive- und Redo-Logs der Datenbanken. Ohne detaillierten Einblick in der Applikationslandschaft und deren Zusammenhänge geht gar nichts.

Das sind die Szenarien, für die man die mehrfach abgesicherten Speichersy-

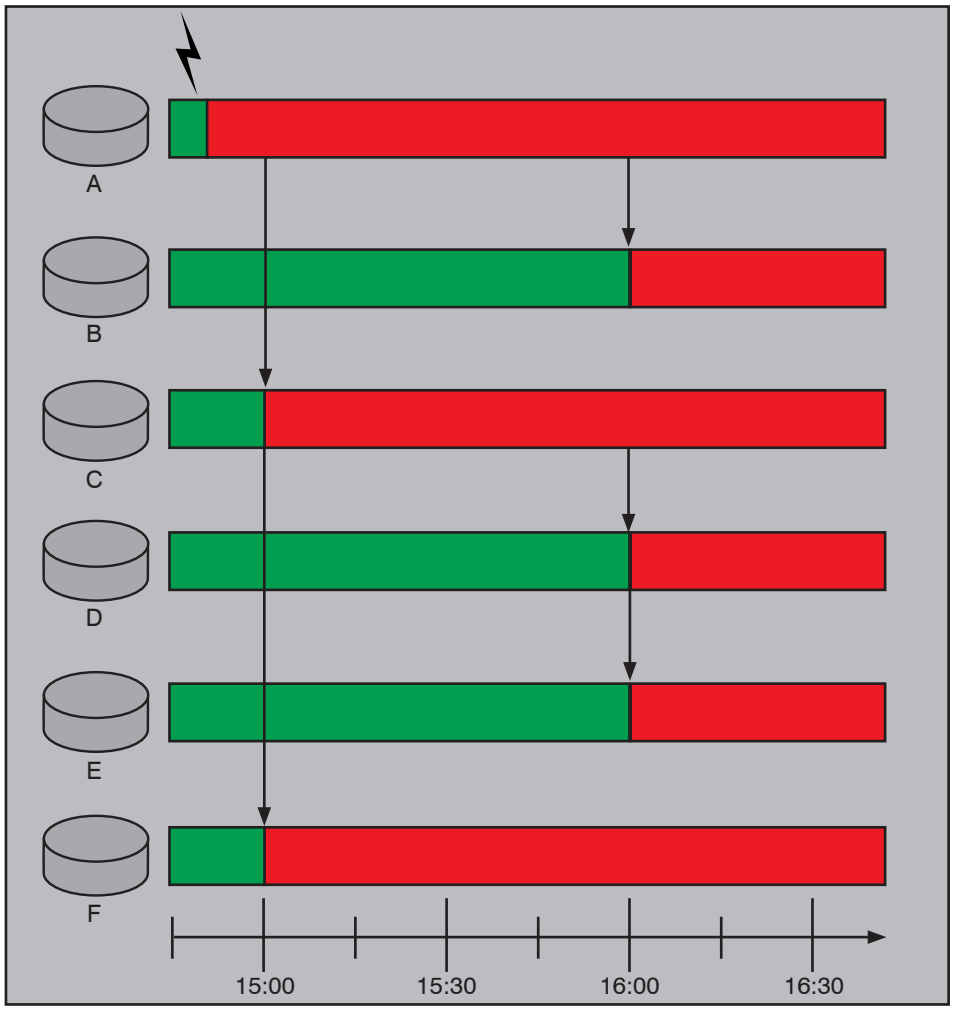


Abbildung 4: Fortpflanzung eines Datenbankproblems

steme, Backup-Strukturen, aber auch Expertise und gute Dokumentation benötigt.

Hilft die Verlagerung von Daten in die Storage Cloud, solche Probleme besser zu beherrschen? Der Autor wagt, das stark zu bezweifeln.

Was bewirkt die Verlagerung in die Storage Cloud?

Was bewirkt die Verlagerung in die Storage Cloud? Was passiert mit den Daten, und wie werden die Einsparungen erzielt? Ein Blick auf die Dienstspezifikation eines Storage-Cloud-Anbieters gibt die Antwort (der Name des Anbieters ist nicht wichtig, da alle Anbieter mehr oder weniger ähnliche Dienste im Portfolio haben):

- Über einen Zeitraum von zwei Jahren wird der Vertrag abgeschlossen, der mit der Entrichtung eines monatlichen Betrages für eine bestimmte Datenmenge verbunden ist.

- Gegen eine Zusatzgebühr kann man (nicht bei allen Anbietern) eine Flat Rate erhalten, bei der das Verkehrsvolumen für Upload und Download unbegrenzt ist, d. h. bis zur vereinbarten Obergrenze können die Daten beliebig oft überschrieben bzw. heruntergeladen werden. Dies ist sehr wichtig, weil die volumenabhängige Abrechnung der Up- und Downloads die Kosten für Cloud Storage durchaus in ungeahnte Höhen steigen lassen kann.

- Der Provider sorgt für die Datensicherung, der Kunde bestimmt die Zeitpunkte der Datensicherung in der Cloud.

- Auf die Daten kann mittels solcher Protokolle wie CIFS/SMB, FTP oder HTTPS zugegriffen werden.

Nun stelle man sich vor, der Betreiber der in der Abbildung 3 dargestellten IT-Umgebung schließt einen solchen Vertrag über Cloud Storage ab. Die Nutzung der Cloud Storage ist in der Abbildung 5 dargestellt.

Unabhängig von der Nutzung eigenen Speichers oder des Speichers in der Cloud muss das Unternehmen in der Lage sein, solche Probleme wie am Beispiel der Datenbanken dargestellt zu lösen. Die Vorstellung, der Storage Provider würde sich um solche Probleme kümmern, ist völlig illusorisch. Was der Storage Provider tut, ist nichts anderes als die Reservierung von Speicherbereichen in der eigenen Infrastruktur für die verschiedenen Systeme des Kunden. Die Wechselbeziehungen zwischen diesen Systemen sind für den Storage Provider irrelevant bzw. ihm nicht bekannt. Wenn solche Zusammenhänge zwischen den Systemen zur Fortpflanzung von Problemen führen, kann der Storage Provider nicht helfen. Er kann zwar die Daten regelmäßig sichern, aber in aller Regel nach einem standardisierten Zeitraster, vielleicht differenziert nach verschiedenen Modellen, jedoch nicht beliebig individualisiert und maßgeschneidert.
Auch wenn die Daten in der Cloud liegen, muss die administrative Hoheit darüber häufig genug vom Kunden selbst wahrgenommen werden. Nur der Kunde ist in der Lage, den Gesamtzusammenhang zwischen den Systemen mit ihren Daten zu überblicken und bei übergreifenden Problemen eine Lösung herbeizuführen. Insbesondere solche Aspekte wie hierarchisches Speichermanagement, Information Lifecycle Management, Datensicherung und Archivierung erhöhen die Komplexität der Zusammenhänge zwischen verschiedenen Systemen und Speichermedien.

Diverse Studien belegen, dass die Kosten für die Speicherinfrastruktur eines Unternehmens nur zu einem eher kleinen Anteil aus den Kosten bestehen, welche bei einer Verlagerung in die Wolke entfallen würden, nämlich die Kosten für die Beschaffung und Unterhaltung des Massenspeichers selbst. Höhere Kosten werden verursacht durch die Administration der Daten und die Datensicherung. Mit einer Verlagerung der Daten in die Wolke verschwindet der Aufwand des Unternehmens bei der Administration der Daten und insbesondere des Backup keineswegs. Es sei denn, die Datensicherung würde für alle Daten konsistent durchgeführt werden können, mit Betonung auf „alle“ und „konsistent“.

Wann ist Cloud Storage sinnvoll?

Der Autor bestreitet nicht, dass es einen realen Markt für Cloud Storage gibt und die Nutzung der Dienste aus diesem Markt manchmal sinnvoll ist. Die hier aufgestellte These ist die folgende: Bei einem komplexen Wechselwirken zwischen verschiedenen Datenbeständen löst Cloud Storage keines der wichtigsten Probleme, die Unternehmen mit ihrer eigenen Speicherinfrastruktur haben.

Nichtsdestotrotz sind Szenarien denkbar, in denen die Nutzung von Cloud Storage durchaus sinnvoll sein kann. Wenn zum Beispiel Speicher in der Wolke als eine von mehreren Speicherklassen gilt und dazu dient, die Wahrscheinlichkeit von Datenverlusten weiter zu reduzieren, ist dagegen nichts einzuwenden. Insbesondere für unstrukturierte Datenbestände, die keinerlei komplexe Zusammenhänge mit anderen Daten haben, kann die Erweiterung der verfügbaren Speicherklassen um Cloud Storage durchaus sinnvoll sein, wenn die eigene Speicherinfrastruktur allein die Anforderungen an die Verfügbarkeit der Daten oder Compliance-Anforderungen nicht erfüllt.

Ferner sind die erweiterten Dienste im Sinne unserer obigen Definition und der Abbildung 2 durchaus sinnvoll, wenn sie mit der Verlagerung einer ganzen Applikation in die Wolke verbunden sind. Neu ist der Ansatz nicht. Spätestens mit dem

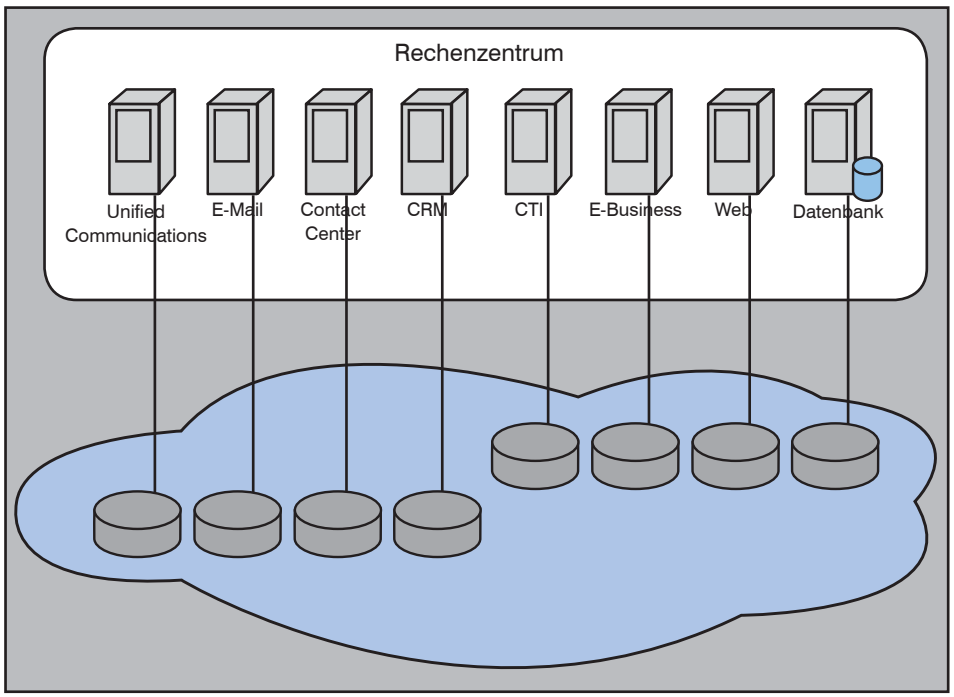


Abbildung 5: Nutzung der Cloud Storage

Cloud Storage: wer braucht das überhaupt?

durchaus erfolgreichen BlackBerry-Dienst hat die Firma RIM bewiesen, dass es auch für Unternehmen interessant sein kann, einen Dienst aus der Wolke zu beziehen. Vergleichbares kann bei Applikationen der Fall sein, die auf neuen Endgeräten wie iPhone oder iPad laufen. Speziell diese Apple-Endgeräte haben (bisher) kein für den Nutzer zugängliches File System, sodass auf solchen Geräten laufende Anwendungen, die den Zugang zu einem File System erfordern, eine Serverkomponente benötigen. Sollen die Endgeräte beliebig mobil sein, sollte die Serverkomponente am besten über das Internet erreichbar sein. Der Dienst Dropbox ist ein Beispiel dafür, wie der Bedarf an File Services für iPhone und iPad abgedeckt werden kann.

Große Hoffnungen setzen die Cloud-Anbieter auch auf kleine Unternehmen, Freiberufler und private Anwender, die durch Nutzung von Cloud Storage die Verfügbarkeit ihrer Daten wesentlich erhöhen können. Ein Beispiel ist eine Arztpraxis: Häufig nutzen Ärzte eine einzige, hoch spezialisierte Datenbank mit zugehörigen Applikationen. Ohne Cloud Storage müsste sich jeder Arzt um die Sicherung seiner Daten kümmern. In vielen Praxen beträgt der Aufwand für die Administration und die Sicherung der Daten, die Pflege der Sicherungsmedien und wichtige Restore Tests mehrere Stunden pro Woche. Gelingt es, durch eine tägliche Sicherung der Daten in die Cloud den Aufwand für die Datenadministration um wenige Stunden pro Monat zu reduzieren, amortisiert sich der zwei- bis dreistellige Betrag, den der Arzt für Cloud Storage entrichten muss.

Aber für die meisten mittleren bis großen Unternehmen ist Cloud Storage kein Allheilmittel. Die kritischsten Daten dieser Unternehmen weisen in der Regel derart komplexe Zusammenhänge auf, dass die eigentliche Beherrschung der Daten wesentlich mehr Aufwand und Sorge verursacht als die dagegen sehr einfache Verlagerung von Daten in die Wolke verändern kann.

So ist in den meisten dieser Unternehmen die Situation im Speicherbereich mit der Situation bei den eigenen Kommunikationsanwendungen vergleichbar. Will jemand nur telefonieren, kann er auf eine eigene Telefonanlage verzichten. Der Dienst kann aus der Wolke kommen. Sind komplexe Beziehungen zwischen den eigenen Verzeichnisdiensten, den E-Mail-Servern, dem Call Center, den Office-Applikationen, den Webinhalten und der Telefonanlage eingerichtet, kommen solche Dienste wie Centrex kaum infrage. Die Wolke ist für solche Umgebungen zu einfach gestrickt.

Vertragliche und Sicherheitsbedenken

Ist die Wolke vertrauenswürdig? Das ist eine Frage, welche die meisten Bedenkenträger gegen Cloud Services beschäftigt. Kann man in doppeltem Sinne dem Provider vertrauen:

- dass er meine Daten immer verfügbar hält und nicht (zum Beispiel durch Arbeitsfehler, die auch beim Provider passieren können) verliert bzw. zerstört, und
- dass er meine Daten vor dem Zugriff durch Unbefugte schützt und alle gesetzlichen Anforderungen an Datensicherheit und Datenschutz erfüllt?

Cloud-Anbieter verweisen natürlich auf ihre Service Level Agreements (SLAs). Aber eine Reihe von Anbietern lässt nicht mit sich verhandeln. Der Kunde hat diese SLAs zu akzeptieren. Zusagen über hohe Verfügbarkeiten sind mit Vorsicht zu genießen, da die Vertragsstrafen aus einer leichten Reduzierung der monatlichen Gebühren bestehen. Im Prinzip tut es einem solchen Provider also nicht weh, wenn mal eine Zusage nicht eingehalten wird.

Auch wenn die Provider zum Beispiel den Kunden in der Europäischen Union zusichern, dass die Daten in Rechenzentren innerhalb der EU gehalten werden und somit nicht gegen europäische Richtlinien verstoßen wird, wenn kritische (zum Beispiel personengebundene) Daten in die Wolke verlagert werden, sehen viele Cloud Services diesbezüglich kritisch. Wie vielen Patienten ist es gleichgültig, ob der Arzt aus unserem oben genannten Beispiel die Patientenakte bei sich behält oder in die Wolke verlagert?

Diese vertraglichen und Sicherheitsbedenken gelten für alle Typen von Cloud Services (ob nur Storage-Basisdienste oder um die Applikation erweitert) und für Unternehmen aller Größen, von der Arztpraxis bis zum Automobilhersteller.

Last but not least: Beim Vergleich zwischen den Kosten für eigenen Speicher und Cloud Storage sollten nicht Äpfel mit Birnen verglichen werden. Ein gespiegeltes und mehrfach abgesichertes Speichersystem hat seinen Preis. Auch in Eigenregie kann man durch Nutzung von Open Source und iSCSI Speicherstrukturen schaffen, die in ihrem Preisniveau weit unter den High-End-Systemen der kommerziellen Anbieter liegen. Die Vermutung liegt nahe, dass einige Storage Cloud Provider genau solche Strukturen für den Massenmarkt nutzen.

Fazit

Allen Cloud Services ist gemeinsam, dass sich der Kunde auf den Provider verlässt. Der Kunde verlässt sich vor allem darauf, dass die Daten beim Provider gut aufgehoben sind, den gesetzlichen Bestimmungen entsprechend, und dass die Abläufe und Mechanismen in der Cloud für die Wahrung der Verfügbarkeit, der Integrität und der Vertraulichkeit der Daten sorgen. In den SLAs vorgesehene Vertragsstrafen reichen häufig als Wiedergutmachung bei Datenverlusten oder Verstößen gegen den Datenschutz und die Datensicherheit nicht aus.

Ferner weisen die IT-Anwendungen der meisten mittleren bis großen Unternehmen derart komplexe Wechselwirkungen auf, dass die Unternehmen im Zusammenhang mit den Daten dieser Anwendungen und den von ihnen belegten Speichersystemen viele Administrations- und Management-Aufgaben selbst wahrnehmen müssen und von einer Verlagerung der Daten in die Wolke nicht wesentlich profitieren.

Die meisten sinnvollen Szenarien für die Nutzung von Cloud Services sind solche, in denen nicht nur die reine Nutzung von Speicherplatz, sondern die Inanspruchnahme von erweiterten Diensten einschließlich Applikation und Storage im Vordergrund steht.

Für die reinen Storage-Basisdienste kann es aber auch sinnvolle Verwendungen insbesondere bei kleinen Unternehmen geben, wenn Cloud Storage als redundante Erweiterung des eigenen Speichers genutzt wird oder es sich nicht um komplex miteinander verknüpfte Datenbestände handelt, die in der Regel unter hohem Aufwand konsistent gehalten werden müssen.

Kongress

ComConsult Storage-Forum 2011
13. - 15.07.11 in Bonn

Das ComConsult Storage-Forum 2011 analysiert die aktuellen Entwicklungen im Speichermarkt, vergleicht Alternativen und zeigt auf, wo der Weg hingeht.

Moderatoren:
Dipl.-Inform. Matthias Egerland,
Dr. Franz-Joachim Kauffels
Preis: € 1.990,-- zzgl. MwSt.

Buchen Sie über
www.comconsult-akademie.de

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Sicherer Internetzugang, 11.04. - 13.04.11 in Aachen

Das Internet hat sich zu der entscheidenden Plattform für moderne Kommunikation und Geschäftsfelder entwickelt – trotz aller mit der damit verbundenen weitgehend unkontrollierten globalen Vernetzung einhergehenden Bedrohungen für IT-Infrastruktur und Daten. Der Anschluss an dieses Kommunikationsmedium muss daher so gestaltet sein, dass unkalkulierbare Risiken vermieden werden, ohne Nutzungspotenziale zu verschenken. Dieses Seminar identifiziert die wesentlichen Gefahrenbereiche und zeigt effiziente und wirtschaftliche Maßnahmen zur Umsetzung einer erfolgreichen Lösung auf. Alle wichtigen Bausteine werden detailliert erklärt und anhand praktischer Projektbeispiele und Übungen wird der Weg zu einer erfolgreichen Sicherheits-Lösung aufgezeigt.

Preis: € 1.890,-- zzgl. MwSt.

Lokale Netze für Einsteiger, 11.04. - 15.04.11 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,-- zzgl. MwSt.

Interne Absicherung der IT-Infrastruktur, 02.05. - 04.05.11 in Köln

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,-- zzgl. MwSt.

TCP/IP intensiv und kompakt, 02.05. - 04.05.11 in Köln

LAN-, WLAN- und WAN-Netzwerke sind heutzutage IP-Netze, und ein Verzicht auf Nutzung des IP-basierten Internet undenkbar. Auch für früher nur mit herstellerspezifischen Protokollen in Verbindung gebrachte Anwendungsgebiete wie Telefonie oder Produktionsumgebungen gibt es mittlerweile geeignete IP-basierte Lösungen. Hersteller und Dienstanbieter versuchen den Eindruck zu vermitteln, die Nutzung sei kinderleicht, fast schon plug and play - man trägt ein paar Adressen ein (wenn überhaupt), und es kann losgehen. Falsch! Preis: € 2.490,-- zzgl. MwSt.

E-Mail-Archivierung planen, evaluieren, umsetzen, 16.05. - 18.05.11 in Bonn

Dieses Seminar behandelt einerseits die rechtlichen Vorschriften zur Speicherung von E-Mails und anderen digitalen Dokumenten sowie die zahlreichen Regelungen zur Beschränkung des Zugriffs auf die Daten aus Gründen des Persönlichkeitsrechts, des Fernmeldegeheimnisses, des Schutzes von Betriebsgeheimnissen und des Datenschutzes. Preis: € 1.890,-- zzgl. MwSt.

Internetworking: optimales Netzwerk-Design mit Switching und Routing, 16.05. - 20.05.11 in Aachen

Dieses 5-tägige Seminar vermittelt Netzwerkbetreibern und Planern Methoden und Technologien zur erfolgreichen Strukturierung von Enterprise Netzwerken. Dabei wird das komplette Spektrum vom L2/L3 Switching über Redundanz/Routing bis hin zu Themen wie VLAN, WLAN-Integration, Multicast-Routing, VPN, MPLS, abgedeckt.Es werden sowohl die theoretischen Hintergrundkenntnisse als auch die Konsequenzen für den praktischen Betrieb von Netzwerken dargestellt. Fallstudien und Gruppenübungen mit Planungsbeispiel vermitteln Informationen, die in der Praxis sofort umgesetzt werden können. Preis: € 2.490,-- zzgl. MwSt.

Trouble Shooting in vernetzten Infrastrukturen, 17.05. - 20.05.11 in Aachen

Dieses Seminar vermittelt, welche Methoden und Werkzeuge die Basis für eine erfolgreiche Fehlersuche sind. Es zeigt typische Fehler, erklärt deren Erscheinungsformen im laufenden Betrieb und trainiert ihre systematische Diagnose und die zielgerichtete Beseitigung. Dabei wird das für eine erfolgreiche Analyse erforderliche Hintergrundwissen vermittelt und mit praktischen Übungen und Fallbeispielen in einem Trainings-Netzwerk kombiniert. Die Teilnehmer werden durch dieses kombinierte Training in die Lage versetzt, das Gelernte sofort in der Praxis umzusetzen. Preis: € 2.290,-- zzgl. MwSt.

IP-Wissen für TK-Mitarbeiter, 23.05. - 24.05.11 in Königswinter

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: € 1.490,-- zzgl. MwSt.

IPv6: Planung, Migration und Betrieb, 30.05. - 01.06.11 in Bonn

Der Wechsel von IPv4 auf IPv6 wird für die meisten Unternehmen und Behörden in den nächsten Jahren unvermeidbar kommen. Dabei liefert IPv6 nicht nur ein neues Adress-Konzept sondern auch ein völlig verändertes Betriebs-Szenario. DHCP und auch DNS müssen neu durchdacht werden. Naturgemäß sind auch Firewall-Installationen und NAT von einer IPv6-Umstellung betroffen. In diesem Seminar erfahren Sie, wo sich mit einer IPv6-Einführung etwas ändert, und wie Migrationsphase und Betriebsalltag aussehen.

Preis: € 1.890,-- zzgl. MwSt.

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze
11.04. - 15.04.11 in Aachen
12.09. - 16.09.11 in Aachen
05.12. - 09.12.11 in Aachen

TCP/IP intensiv und kompakt
09.05. - 13.05.11 in Königswinter
26.09. - 30.09.11 in Stuttgart

Internetworking
16.05. - 20.05.11 in Aachen
17.10. - 21.10.11 in Aachen

Paketpreis für alle drei Seminare € 6.720,-- zzgl. MwSt. (Einzelpreise: je € 2.490,--)

ComConsult Certified Trouble Shooter

Trouble Shooting in vernetzten Infrastrukturen
17.05. - 20.05.11 in Aachen
20.09. - 23.09.11 in Aachen

Trouble Shooting für Netzwerk-Anwendungen
28.06. - 01.07.11 in Aachen
18.10. - 21.10.11 in Aachen

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

ComConsult Certified Voice Engineer

Session Initiation Protocol Basis-Technologie der IP-Telefonie
27.06. - 29.06.11 in Hamburg
14.11. -16.11.11 in Bonn

Sicherheitsmechanismen für Voice over IP
04.07. - 05.07.11 in Nürnberg
17.11. - 18.11.11 in Aachen

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen
06.06. - 08.06.11 in Nürnberg
26.09. - 28.09.11 in Stuttgart
28.11. - 30.11.11 in Köln

Basis-Paket: Beinhaltet die drei Basis-Seminare
Grundpreis: € 4.740,-- zzgl. MwSt. statt € 5.270,-- zzgl. MwSt.

Optionales Einsteigerseminar: Aufpreis € 1.090,-- zzgl. MwSt. statt € 1.490,-- zzgl. MwSt.

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
23.05. - 24.05.11 in Königswinter
10.10. - 11.10.11 in Berlin

Impressum

Verlag:
ComConsult Technology Information Ltd.
ComConsult Research
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

Für unverlangte eingesandte Manuskripte
wird keine Haftung übernommen
Nachdruck, auch auszugsweise
nur mit Genehmigung des Verlages
© ComConsult Research