ComConsult Research

Der Netzwerk Insider

Februar 2012

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

Bring your own Device - Vorbote eines Umbruchs in der IT

von Dr. Simon Hoff, Dominik Zöller

Mit Bring Your Own Device (BYOD) erleben wir im Moment einen Trend, von dem immer deutlichere Signale ausgehen, dass hier ein Umbruch der gesamten IT seinen Anfang genommen hat. Mit BYOD drängen mit Macht privat genutzte bzw. fremde Endgeräte, insbesondere Smartphones und Tablets, die ursprünglich primär für den Consumer-Markt geschaffen wurden, in die IT. Dieser Artikel beschreibt die Techniken, die für eine sichere Unterstützung von BYOD notwendig sind, und analysiert die Möglichkeiten und Grenzen der verfügbaren Produkte.

1. IT Consumerization und die Folgen

Die Antike der IT, in der innovative Technologien zuerst Unternehmen zur Verfügung standen, bevor sie anschließend den Privatsektor eroberten, ist Geschichte. Heute wird Innovation verstärkt durch Konsumentenmärkte getrieben. Die Anwender tragen ihre Erwartungshaltung an Leistungsfähigkeit und Bedienbarkeit von Applikationen und Endgeräten in das Unternehmen.

weiter auf Seite 11

Zweitthema

Funktionsreichtum kontra Vereinfachung

von Dr. Behrooz Moayeri

Aus unserem Kundenkreis bekommen wir bezüglich der Konzipierung von Local Area Networks zwei widersprüchliche Arten von Signalen: einerseits die Nachfrage nach immer mehr LAN-Funktionen in verschiedenen Bereichen (Security, QoS, Energiemanagement, ...) und andererseits die Botschaft, dass angesichts der zunehmenden Anforderungen an die LAN-Verfügbarkeit und vor dem Hintergrund knapper Personalressourcen ein robustes, möglichst einfach aufgebautes LAN gefragt sei.

Dieses Dilemma ist nicht neu. Seit mindestens 15 Jahren diskutieren wir mit unseren Kunden über die Frage, wie viel Funktionsreichtum ein LAN verkraftet, das jahrelang zuverlässig arbeiten und betrieben werden muss. Der Autor erinnert sich immer wieder an den Leitsatz eines unserer Kunden: „Komplex wird das LAN im Laufe der Jahre ohnehin; man braucht nicht auch noch komplex anfangen. “Dieser Spruch lässt sich durchaus wissenschaftlich mit dem Entropiegesetz fundieren.

weiter auf Seite 20

Aktuelle Kongresse

ComConsult Netzwerk-Redesign Forum 2012
ComConsult IPv6-Forum 2012

ab Seite 5

Geleit

Bring Your Own Device

auf Seite 2

Standpunkt

Sicherheitsrisiko Firewall

auf Seite 19

Neues Seminar

Anwendungs-Virtualisierung für Android, iPad & Co

auf Seite 18

Zum Geleit

Bring Your Own Device

Die Nutzung mobiler Endgeräte nimmt explosionsartig zu. Stärkere Prozessoren, mehr Speicher und eine gute Grafik gestatten die Nutzung auch komplexer Applikationen auf einem mobilen Endgerät, sei es ein Smartphone oder ein Tablet. Spätestens die letzten Verkaufszahlen von Apple zeigen, dass wir in sehr kurzer Zeit mit einer weiteren und schnellen Zunahme dieser Geräte in den Unternehmen rechnen müssen. Der weltweit diskutierte Mega-Trend ist dabei die Nutzung privater Geräte für Unternehmens-Anwendungen: Bring-Your-Own-Device BYOD. Was auf den ersten Blick wie eine geniale Möglichkeit wirkt, Interessen von Mitarbeitern und Unternehmen in einer typischen Win-Win-Situation gleichermaßen zu befriedigen, generiert bei näherer Betrachtung erhebliche betriebliche und auch wirtschaftliche Probleme.

Für viele Mitarbeiter ist BYOD interessant. Zwar übernehmen sie quasi Investitionen für das Unternehmen aus eigener Tasche. Häufig können sie jedoch auf diese Weise die zu engen Regeln für Unternehmens-eigene Geräte umgehen und moderne Geräte und Applikationen nutzen. Betrachtet man die Zahl der Unternehmen mit mehr als 5 Jahre alten PCs und Internet Explorer 6, dann ist jeder Weg, diesem Technologie-Museum zu entgehen für die Mitarbeiter ein Fortschritt.

Für die Unternehmen ergeben sich auf den ersten Blick erhebliche Einsparungen im Invest-Bereich, da die Mitarbeiter ja die Kosten der Anschaffung tragen. Tatsächlich motiviert gerade dieser Aspekt offenbar viele Führungskräfte BYOD als interessant zu sehen und zu puschen.

Bei näherer Betrachtung hat BYOD je nach Art und Umfang der Nutzung im Unternehmen eine ganze Reihe von Nachteilen:

- beginnen wir mit der Idee der Einsparung. Die ist natürlich grober Unfug. Für alle IT-Geräte spielt die Höhe der Betriebskosten eine erhebliche Rolle. Diese sinken nicht dadurch, dass mobile Geräte zum Einsatz kommen. Vielmehr ist zu befürchten, dass je nach genutzten Anwendungen die Betriebskosten im Sinne von Service-Leistungen steigen. Gerade bei scheinbar preiswerten Geräten ist das kritisch, da die Betriebskosten schnell die Anschaffungskosten übersteigen. Die einfache Regel ist: je preiswerter ein Endgerät

ist, desto mehr sind die Betriebskosten entscheidend.

- dann kommen wir zur Frage der genutzten Applikationen. Email können wir als überschaubar ansehen, auch wenn je nach genutztem Gerät ein IMAP-Gateway erforderlich wird, das gegebenenfalls ansonsten nicht zum Einsatz käme. Aber schon bei der mobilen Bearbeitung von Texten beginnen die Probleme. Das reine Lesen ist ok, aber wenn es darum geht, Text zu ändern oder zu kommentieren, ist das nicht ganz trivial. Zwar werben diverse Apps mit der Kompatibilität zu Microsoft Office, aber hier liegen die Tücken im Detail. Auch wenn die Apps immer besser werden, unsere Tests zeigen je nach Dokument weiterhin Probleme. Und wer die Idee hat, diese Dokumente nach der Veränderung wieder ins Unternehmen zurück zu übertragen, der sollte besonders vorsichtig sein. PDF ist lösbar, allerdings ist darauf zu achten, dass bei der Rück-übertragung ins Unternehmen Anmerkungen oder Markierungen erhalten bleiben. Schon an diesen Beispielen wird klar, dass wir hier auf ein Service-Minenfeld stoßen. Wer dies nicht sauber vorbereitet, wird schnell deutlich mehr Geld für Personal oder Beratung ausgeben, als er bei der Beschaffung der Geräte einsparen würde.

- auch die Frage, wie Daten eigentlich zu

Abbildung 1: Vertriebsunterstützung auf dem iPad Quelle: Apple

den Geräten und wieder zurück ins Unternehmen kommen, ist spannend. Der übliche Weg ist durch die Nutzung von Webdiensten wie Dropbox oder SugarSync. Auch der mehr professionelle Dienst von Box.Net erfährt eine immer weitergehende Akzeptanz. Zum einen entstehen damit erhebliche Kosten und Probleme in der Benutzerverwaltung (die meisten dieser Cloud-Dienste sind nicht auf Unternehmens-Anforderungen ausgelegt und skalieren in der Benutzerverwaltung nicht gut, alleine die Möglichkeit der Bildung von Gruppen ist bisher selten vorhanden). Damit nicht genug, entsteht damit die Grundsatzfrage der Nutzung von Cloud-Diensten. Und die hat wie schon häufiger diskutiert nicht ganz unerhebliche Tücken.

- muss man aus Unternehmenssicht Sandboxing als K.O.-Kriterium fordern? Wenn ja, was ist dann mit Android? Und wie sind die Schnittstellen zwischen Apps. zu bewerten, über welche die Daten zwischen den Sandboxes weitergegeben werden können? Und hat Sandboxing nicht auch Nachteile? Immerhin entstehen durch das fehlende zentrale Dateisystem schnell verschiedene Versionen derselben Datei in verschiedenen Apps. Welche gilt denn jetzt und von wo aus wird ins Unternehmen zurück übertragen?

- damit sind wir bei den Geräten selbst. BYOD ist ja schön, aber das kann ja wohl kaum heißen, dass jedes mobile Endgerät seitens des Unternehmens unterstützt wird. Android ist mit seinen vielen Versionen und Hersteller-spezifischen Erweiterungen ein Service-Grab für Unternehmen. Aber auch bei Apple stellt sich mindestens die Frage, welche iOS-Version unterstützt werden soll. Immerhin gibt es erhebliche Funktionsunterschiede zwischen den Versionen.

- bedeutet BYOD eigentlich, dass das Unternehmen keine Investitionen zu tätigen hat, da ja die Mitarbeiter alles bezahlen? Sicher nicht. Die WLAN-Infrastruktur muss erheblich aufgerüstet werden. IEEE 802.11n reicht mittelfristig nicht aus. Aber was wird der Folgedienst? Wie kommen Daten zu und von den Geräten, braucht das Unternehmen private Cloud-Dienste? Wie greifen Mitarbeiter von Außen auf diese Cloud-Dienste zu? Sind diese Dienste als virtuelle Maschinen aufgesetzt? Wie wird welcher Speicher eingebunden? Wird Redundanz über verteilte Rechenzentren geschaffen? Reicht dann normales Routing zum Zugang aus oder werden neue Lösungen wie LISP von Cisco gerade in diesem Umfeld unverzichtbar? Was ist mit IPv6? Sollte nicht gerade eine neue Gerätewelt von vornherein daran ausgerichtet sein? Was ist dann mit Routern und Firewalls, nach wie vor ist die Liste der Geräte, die nicht IPv6-fähig sind sehr lang? Wo laufen Profile Manager, die brauchen doch eigentlich eigene Server, die sollten redundant und nach Möglichkeit verteilt sein. Schon auf den ersten Blick ist BYOD ohne deutliche Investitionen auf der Unternehmensseite nicht umsetzbar. Dabei darf auch der Know-How-Aufbau für das Betriebspersonal nicht unterschätzt werden. Wer bisher keine Apple-Welt kennt, der wird sich zu Beginn mit dem Profil Manager auf Mac OS Lion Server schwer tun (ein Produkt mit extrem vielen Problemen).

- BYOD generiert ein gewaltiges Sicherheitsproblem. Sollen die mobilen Geräte auf normale Unternehmens-Anwendungen und Daten zugreifen, dann können sie nicht als Gastgeräte im WLAN behandelt werden. Die Rechte eines normalen Desktops möchte man ihnen eigentlich auch nicht geben. Im Prinzip entsteht der Bedarf für eine ganz neue Zonenkonstruktion. Immerhin gibt es auch für mobile Geräte massenweise Tools zur Abhörung des Netzwerkes, zum Zugang auf Server und Anwendungen etc. Das Sicherheitsproblem ist ernst zu nehmen. Auch Keylogger auf mobilen Geräten können zu einem Problem werden. Die Liste der zu diskutierenden Punkte ist lang. Inwieweit sind Passwortdienste erforderlich? Wie sieht es mit Zertifikaten aus? Reicht Remote-Wipe? Ist "Find-My-iPhone" eigentlich aus Betriebsratssicht eine zulässige und gewünschte Funktion?

Die alles entscheidende Kernfrage ist allerdings, wer die Betriebshoheit über die BYOD-Geräte erhält. Sind Mitarbeiter bereit und gewillt, ihre privaten Geräte der Entscheidung des Unternehmens zu unterwerfen? Was ist mit der Installation neuer Apps? Wer entscheidet hier, was erlaubt ist und was nicht? Was ist mit der Nutzung von Cloud-Diensten? Was für das Unternehmen ein großes Problem darstellen kann, ist für die Mitarbeiter ein wesentlicher Teil der Attraktivität der mobilen Geräte. iCloud von Apple oder Applikationen wie PhotoSync und auch das schon angesprochene Dropbox sind aus privater Sicht fast unverzichtbar. Im Prinzip kann es dabei kaum einen sinnvollen Kompromiss geben.

Aber nehmen wir mal an, das Unternehmen soll die Hoheit bekommen, mit welchen Tools wird der Betrieb durchgeführt? Apple hat den Profile-Manager und damit theoretisch einen klaren Marktvorsprung. Aber der Profile-Manager deckt wesentliche Aufgaben nicht komplett ab, die dann nur lokal händisch ausgeführt werden können (zum Beispiel Backup).

Abbildung 1: Kernfunktion Kollaboration, hier mit WebEx Quelle: Apple

Abbildung 2: Typisches Beispiel für einen völlig neuen Typ von Applikation, iBookAuthor, ohne Frage ein Meilenstein Quelle: Apple

Auch erfordert er den Lion-Server, der nicht wirklich eine Bereicherung darstellt. Der Apple Server war immer schon eine unglückliche Mischung aus einer komfortablen Oberfläche und vielen Zusatzfunktionen, die nur auf Command-Line gehen. Auch müssen zum Teil Linux-Tools nachinstalliert werden, wenn vorhandene Dienste nicht ausreichen. Mit Lion ist das noch schlimmer geworden. Hoffen wir, dass die nächsten Release-Stände zu einer Verbesserung führen. Natürlich kann man auch auf kommerzielle Produkte von Drittanbietern zugreifen, aber die sind auch in einer Frühpase der Entwicklung. Wir werden dies in unserem BYOD-Seminar ausführlicher diskutieren.

In jedem Fall ist davon auszugehen, dass mobile Endgeräte auch neue Formen von Anwendungen mit sich bringen werden, die bisher so noch nicht existieren. Im Gesundheits- und Transport-Bereich ist das klar zu sehen und auch Universitäten und Schulen gehen neue Wege mit mobilen Endgeräten, speziell dem iPad. Alle Unternehmen müssen sich die Frage stellen, welche Konsequenz diese Geräteklasse für Kollaborationsanwendungen haben wird. Es ist absehbar, dass speziell dieser Funktionsbereich in Zukunft eine große Rolle auf mobilen Endgeräten spielen wird. Das Avaya Flare und Cisco Cius sind weitergehende Beispiele für diesen Trend. Aber auch bekannte Apps wie FuzeMeeting und WebEx unterstreichen das.

Damit sind wir bei Pro und Kontra-Standpunkten zu BYOD.

Die Pro-Sicht
Mitarbeiter können moderne Geräte ihrer eigenen Wahl nutzen und müssen nicht Jahre warten bis sich ihre IT dazu durchringt das nach langen Diskussionen zu machen. Unternehmen erhalten zufriedene Mitarbeiter und sparen Anschaffungskosten.

Die Kontra-Sicht
Mobile Endgeräte sind für Unternehmen unverzichtbar. Sie schaffen erhebliche Vorteile auf funktionaler Ebene und machen den Weg in eine ganze Dimension neuer Anwendungen frei. Sie sind ohne Frage strategisch. Auf keinen Fall sollten sie als Spielzeug zum Lesen von Email und einfachen Texten abgetan werden. Strategische Geräte sollten immer vom Unternehmen beschafft werden, dies kann nicht Aufgabe der Mitarbeiter sein. Damit löst sich auch die Frage des Kernkonflikts, wer eigentlich die Entscheidungshoheit über diese Geräte hat. Die kann bei strategischen Geräten nur beim Unternehmen liegen. Aber auch aus der Sicht der Sicherheits-Lösung muss das Unternehmen bei Geräten, die mehr Rechte als ein Gastzugang bekommen, die Hoheit haben. Hinzu kommt, dass die Sichtweise der Einsparung durch BYOD sowieso nicht haltbar ist. Betrachtet man die Folgekosten für geeignete Infrastrukturen und den Betrieb, ist die Frage der Anschaffungskosten fast unerheblich.

Damit ist auch das Fazit klar. Das Fazit ist eine klare Befürwortung der verstärkten Nutzung mobiler Endgeräte. Dies erfordert ein sehr umfassendes Betriebskonzept, will man nicht in einem Service- und Sicherheits-Debakel enden. Dies erfordert auch wichtige und unverzichtbare Entscheidungen zur Infrastruktur. Wie kommen Daten zu den mobilen Geräten hin und wieder zurück? Welche Cloud-Dienste sind akzeptabel, an welcher Stelle müssen Unternehmen eigene Dienste aufbauen? Und einer der wichtigsten Punkte ist der Sicherheitsbereich. Mit oder ohne BYOD erfordern mobile Endgeräte eine Erweiterung der bisherigen Zonenkonzepte.

Ihr
Dr. Jürgen Suppan

Aktueller Kongress

ComConsult Netzwerk-Redesign Forum 2012

23. - 25.04.12 in Bad Neuenahr
26.04.12 Intensiv-Tag "VLAN-Optimierung"

Die ComConsult Akademie veranstaltet vom 23. - 26.04.12 ihr "ComConsult Netzwerk-Redesign Forum 2012" in Bad Neuenahr.

Die explosionsartige Zunahme mobiler Endgeräte und Web-basierter Applikationen verändern unsere IT. Neue Architekturen für den Zugang und den Betrieb der Dienste müssen umgesetzt werden und erfordern weitreichende Änderungen in den Netzwerk-Infrastrukturen. Ohne geeignete Sicherheits-Konzepte auf Netzwerk-Ebene wird das Ganze nicht funktionieren.

Heiß diskutierte Fragen sind dabei:

- Welche Auswirkungen hat die starke Zunahme mobiler Endgeräte?
- Wie stark lassen wir Virtualisierung das Design unserer Netze bestimmen?
- Wie sehen zukünftige Zugangs-Architekturen aus?
- Was muss LAN-Technik machen, um die Voraussetzungen zu erfüllen?
- Was muss sich im WAN ändern? Brauchen wir technisch ein neues Routing-Zugangsverfahren?

Das ComConsult Netzwerk-Redesign Forum unterteilt sich in folgende Themenbereiche:

1. Analyse wesentlicher IT-Trends und Auswirkungen auf Infrastrukturen
2. Mobile Endgeräte und ihre sichere und performante Integration
3. LAN-Technologie und neue Architekturen: wie umfangreich sind die Änderungen?
4. WAN-Zugang zu und zwischen Infrastrukturen: Wie kritisch wird das Thema?
5. Basis-Infrastrukturen und ihr Betrieb
6. Optional buchbarer Vertiefungstag: VLAN-Strukturen: wo ist das Optimum

Dabei gehen wir auf eine Reihe von Streitfragen ein, die den Markt jetzt und in den nächsten Monaten bewegen werden (beobachten Sie die Diskussion auf www.comconsult-research.de).
Beispiele dafür sind:

- Bring Your Own Device: voller Zugang zu Infrastrukturen und trotzdem sicher? Macht Bring-Your-Own-Device technisch und wirtschaftlich Sinn?
- WLAN-Zukunft: 802.11n reicht für die mobile Zukunft nicht aus, aber wo liegt die Zukunft? IEEE 802.11ac kontra IEEE 802.11ad
- Verteilte und virtualisierte Strukturen: welche Konsequenzen hat das für LAN und WAN?
- Was müssen Provider in Zukunft leisten?
- LAN-Architekturen im Streit: brauchen wir die neuen Standards überhaupt, und welche Relevanz haben sie im Campus?
- VLANs zwischen Alptraum und Notwendigkeit: wie viel ist gut, ab wenn beginnt das Chaos?

Das Forum ist wie folgt strukturiert:

- Vorträge mit Top-Referenten und Erfahrungsberichten aus der Praxis
- Neueste Forschungsergebnisse von ComConsult Research für zukunftssichere Investitionen
- Begleitende Ausstellung in Kombination mit einem Vortragswettbewerb zur Präsentation der besten Projekte und Ideen in der Veranstaltung
- Get Together am ersten Tag
- Abschließender Intensiv-Tag mit Vertiefung einzelner Top-Themen

Dies ist unser wichtigster Netzwerk-Kongress des Jahres 2012 mit Top-Themen, die für alle Planer und Betreiber von Netzwerken wichtig sind. Versäumen Sie nicht, sich einen Platz in dieser herausragenden Veranstaltung zu sichern.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

ComConsult Netzwerk-Redesign Forum 2012

Ich buche den Kongress
ComConsult Netzwerk-Redesign Forum 2012
☐ vom 23.04. - 25.04.12 in Bad Neuenahr
zum Preis € 2.090,-- netto

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 12

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

Ich buche den
Intensiv-Tag "VLAN-Optimierung"
☐ am 26.04.12 in Bad Neuenahr
zum Preis € 990,-- netto

_____
Vorname

_____
Firma

_____
Straße

_____
eMail

Ich buche den
Kongress und den **Intensiv-Tag**
☐ vom 23.04. - 26.04.12 in Bad Neuenahr
zum Preis € 2.490,-- netto

_____
Nachname

_____
Telefon/Fax

_____
PLZ,Ort

_____
Unterschrift

Programmübersicht - ComConsult Netzwerk-Redesign Forum 2012

Montag, den 23.04.2012

9:30 bis 10:30 Uhr
Keynote: Infrastruktur für eine grundlegend gewandelte IT
- Was bedeuten die neuen Endgerätetypen für die Infrastruktur?
- Bring Your Own Device (BYOD): Vorbereitung der Infrastruktur auf den Anschluss von Endgeräten unterschiedlicher Vertrauensstufe
- Web-Applikationen: unterschiedliche Varianten und ihre Auswirkung auf die Infrastruk-tur
- Grenzen zwischen Arbeits- und Massenspeicher verschwinden: was bedeuten schnelle Speicher und Prozessoren für die Infrastruktur?
- Ist der Client-Server-Verkehr überhaupt vom Server-Speicher-Verkehr zu trennen?
- Server-Based Computing: Vorteile und Auswirkungen
- Public und Private: Netze für verschiedene Cloud-Varianten
- Wie schnell muss die Infrastruktur auf neue Anforderungen reagieren und wie muss sie dafür aufgestellt sein?

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

10:30 bis 11:15 Uhr
Web-Applikationen und private Cloud-Dienste: unterschiedliche Varianten und ihre Auswirkung auf die Infrastruktur
- Trendanalyse: wo geht es hin
- Typische Nutzungsformen
- Architekturen im Vergleich
- Konsequenzen für Infrastrukturen

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

11:15 bis 11:30 Uhr - Kaffeepause

11:30 bis 12:30 Uhr
Virtualisierungstrends 2012: Die Zukunft des Patchkabels ist virtuell
- Konventionelle Anbindung virtueller Maschinen über den vSwitch
- Historischer Exkurs: „Aufbohren“ des virtuellen Switches durch leistungsfähigere Software (NX1kv)
- Schritt 1: Virtualisierung der Hardware-Schnittstelle (VEB)
- Schritt 2: Durchreichen der virtuellen Schnittstelle an den physischen Switch (VEPA, VN-Link)
- Ausblick: Verschmelzen von physischem Server und Netzwerk: die Hardware-Schnittstelle wird zur Linecard (FabricExtender für Blade-Systeme und Rack-Server); welche nicht zuletzt organisatorischen Herausforderungen bringt dies mit sich?

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

12:30 bis 14:00 Uhr - Mittagspause

14:00 bis 15:00 Uhr
Next Generation IT mit BYOD!?
- Quadratur des Kreises: Mobile Device Management und BYOD
- Caching von Unternehmensdaten in verschlüsseltem Container auf privatem Endgerät - Reichen Sandboxing und Verschlüsselung für BYOD aus?
- Virenausbreitung und BYOD
- Moderne Web-Applikationen + Server-based Computing + BYOD = NGN IT?
- Nicht trivial: WLAN-Architekturen für BYOD
- BYOD im kabelbasierten LAN: Mission impossible?

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

15:00 bis 15:30 Uhr
Mobile Technologien im Unternehmen *N.N.*

15:30 bis 16:00 Uhr - Kaffeepause

16:00 bis 17:00 Uhr
Kollision von Zwiebelschalenmodell und Multi-Mandantennetz
- Wenn Materie auf Antimaterie trifft: Zwiebelschalen-Modelle und Domänen-orientierte Zonenkonzepte à la Microsoft
- Der Client spielt die Musik: Fat Clients, Thin Clients, BYOD, Fremdgeräte und die Auswirkung auf Zonenarchitekturen
- Unter welchen Bedingungen sind mandantenfähige Netze sinnvoll und wann sollte man besser darauf verzichten?
- Projekterfahrungen in der Netzzugangskontrolle: Wenn Wunsch und Realität zusammentreffen
- Filterung an Zonengrenzen: Was leistet eine anwendungsorientierte Filterung und wo sind die Grenzen?

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

17:00 bis 17:30 Uhr
Zonenarchitektur in der Praxis der IKB
- Applikationsvirtualisierung in einer mandantenfähigen Umgebung als Produkt für den Markt
- Aufbau der Zonenarchitektur
- Herausforderungen: Mandantenfähigkeit, Virtualisierung, Administration und IT-Sicherheit
- Projekterfahrungen

Mark Tümpfel, IKB Data GmbH

ab 18:00 Uhr - Get Together

Dienstag, den 24.04.2012 - vormittags

9:00 bis 10:30 Uhr
Wireless LAN Technologie: Update 2012
- Ist 11n am Ende? Wann kommt endlich das Gigabit-WLAN?
- WLAN und IPv6: Was geht, was geht noch nicht?
- Sicherheitsrisiko Heimarbeitsplatz. Die WPS-Panne und wie man damit umgeht.
- Pleiten, Pech und Pannen, Berichte aus der ComConsult-Fehlersuche Praxis
- Die Kompatibilität als Hemmschuh des Fortschritts. Gilt das auch für WLAN?

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

10:30 bis 11:00 Uhr - Kaffeepause

11:00 bis 12:30 Uhr
LAN 2015
- Campus und Data Centre: wie unterschiedlich sind die Anforderungen?
- Network Technology Architecture / Application Connected Framework
- Welche Anforderungen bestehen im Access Bereich, für Einzelswitches und Stacks?
- Wie sieht bei Daten- und Multimedia-Anwendungen die Core-Anbindung des Access Bereichs aus?
- Welche Anforderungen resultieren aus den neuen WLAN Standards?
- Wieviel Tier braucht der Campus und das RZ?
- Wann kann die Aggregation Ebene im Campus wegfallen?
- Wie sieht die moderne Anbindung von RZ und SAN an den Core aus?
- Leistungsparameter Durchsatz/Datenrate, Low Latency und Lossless Delivery: wie viel davon in welchen Bereichen?
- Was sind Video-Ready LANs?
- Switches in Servern
- IEEE 802.1Qbg (EVB) und IEEE 802.1BR (Bridge Port Extension)
- Welche Erfahrungen gibt es mit DCB?
- Wozu braucht man noch Layer 3 in LANs?

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

12:30 bis 14:00 Uhr - Mittagspause

Programmübersicht - ComConsult Netzwerk-Redesign Forum 2012

Dienstag, den 24.04.2012 - nachmittags

14:00 bis 14:40 Uhr
Modernes Layer-2 Design – was kannes, was nutzt es?
- Wie ist die Skalierbarkeit von VLANs im Core und Access Bereich?
- Limitierungen von MST
- Welche Sicherheitsrisiken bedingt der Einsatz von VLANs und wie begegnet man ihnen?
- Welche Verfahren sollten bei welchen Einsatzszenarios genutzt werden?
  - TRILL, VXLAN, NVGRE, OTV, LISP
- Interworking verschiedener Verfahren: PVST, MST, TRILL, VXLAN, LISP

Gerd Pflüger,
Cisco Systems GmbH

14:45 bis 15:25 Uhr
OpenFlow als neues Switchkonzept?
- Was ist SDN und OpenFlow?
- Open Network Foundation (ONF) und OpenFlow Consortium
- Standardisierung
- Internet2 und andere Einsatzszenarien
- Verfügbare Produkte

Axel Simon,
Hewlett-Packard Deutschland GmbH

15:25 bis 16:00 Uhr - Kaffeepause

16:00 bis 16:40 Uhr
SAN Konvergenz; FC vs. FCoE vs. iSCSI mit DCB
- Wo steht beim RZ 2015 der Fibre Channel?
- Verfügbare Bandbreiten, Vorteile, Nachteile, Einsatzszenarien von FC
- Wo steht beim RZ 2015 FCoE?
- Verfügbare Bandbreiten und CNAs, Stand der Standardisierung
- Vorteile, Nachteile, Einsatzszenarien von FCoE
- Wo steht beim RZ 2015 iSCSI?
- Verfügbare Bandbreiten, TCP-Offload NICs, Stand der Standardisierung
- Vorteile, Nachteile, Einsatzszenarien von iSCSI

N.N.,
Brocade Communications GmbH

16:45 bis 17:30 Uhr
TRILL vs. IEEE 802.1Qaq vs. Multi-Chassis Link Aggregierung (MC-LAG)
- IEEE 802.1AXbq
- MC-LAG Konzepte der Hersteller
- Aktueller Stand der Standardisierung bei TRILL
- Aktueller Stand der Standardisierung bei IEEE 802.1Qaq
- Vorteile, Nachteile, Gegensätze
- Wird sich TRILL oder IEEE 802.1Qaq gegen MC-LAG durchsetzen?

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

Mittwoch, den 25.04.2012

9:00 bis 10:15 Uhr
WAN 2015
- Provider Backbone Bridging (PBB) und Provider Shortest Path Bridging (PSPB)
- MPLS versus Ethernet
- Layer 2 versus Layer 3 im WAN
- WAN Optimisation Controller (WOC): sinnvolle Einsatzgebiete, Marktübersicht, Gren-zen und Einschränkungen
- Übertragung von Voice und Video über das WAN

Dr. Behrooz Moayeri,
ComConsult Beratung und Planung GmbH

10:15 bis 11:15 Uhr
RZ-RZ-Kopplung: und jetzt?
- Netzwerk-seitige Anforderungen an heutige RZ-Kopplungen
- Aktiv-Aktiv-Betrieb vs. Desaster-Recovery-Sites: welche Auswirkungen ergeben sich im Netzwerk?
- Verlagerung von Diensten in das 2. RZ oder in die Cloud: wie findet die Netzwerkkommunikation ihr Ziel?
- Optimierung der Verkehrsflüsse durch Trennung von IP-Zielen von ihrem Aufenthaltsort mittels des Locator ID Seperation Protocols (LISP)
- Welche neuen Herausforderungen bringen gekoppelte RZs mit sich?

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

11:15 bis 11:45 Uhr - Kaffeepause

11:45 bis 12:30 Uhr
Serviceprovider im Wandel?
- Anforderungen und Veränderungen aus dem Markt
- Technologien Wired & Wireless - Trends
- Möglichkeiten & Architekturen, die sich daraus für Service Provider ergeben
- Internationale Beispiele

Günter Honisch,
Deutsche Telekom Senior Fellow

12:30 bis 14:00 Uhr - Mittagspause

14:00 bis 14:45 Uhr
Aufbau eines Rechenzentrums nach TIA 942
- Struktur, Inhalte, Ziele
- Abgrenzung zur EN 50173-5
- Was verbirgt sich hinter den Tier-Spezifikationen?
- Wo bietet die Norm eine Hilfe, wo nicht?
- Welche Empfehlungen können gegeben werden?

Dipl.-Inform. Hartmut Kell,
ComConsult Beratung und Planung GmbH

14:45 bis 15:30 Uhr
Netzanalyse/Management/Tools: wie sieht der ideale Mix aus?
- Performance Monitoring, das „Stiefkind“ des Netzbetriebs
- „Schweizer Taschenmesser“ oder Spezialwerkzeuge
- Der ideale Werkzeugkasten für den Betrieb
- Was soll im Monitoring erfasst werden, was nicht?
- Produktivität versus Reaktivität
- Verantwortung, der Schlüssel zum erfolgreichen Netzbetrieb

Dr. Joachim Wetzlar,
ComConsult Beratung und Planung GmbH

15:30 bis 16:15 Uhr
IPv6-Anforderungen an Netzwerk-Komponenten: wo steht der Markt?
- Welche Komponenten sind betroffen?
- Welche Funktionen sind erforderlich?
- Welche Probleme für Projekte entstehen momentan?
- Was bringen Zertifizierungen?
- Wie ist der aktuelle Status für Netzwerkkomponenten?

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

16:15 Uhr Ende der Veranstaltung
Kaffeepause für Teilnhemer am Intensiv-Tag

Der Veranstalter behät sich Ändeurngen im Porgramm vor!

Programmübersicht - ComConsult Netzwerk-Redesign Forum 2012 - Intensiv-Tag

VLAN-Planung: was ist das Optimum? Intensiv-Tag am 26.04.2012

im Anschluss an das ComConsult Netzwerk-Redesign Forum 2012

Donnerstag, den 26.04.2012 - Intensiv-Tag „VLAN-Planung: was ist das Optimum?“

9:00 bis 9:45 Uhr
VLANs: Alptraum oder unverzichtbares Betriebsinstrument?
- Pro: warum VLANs gut sind
- Kontra: warum man auf sie verzichten sollte
- Die Realität: optimale Nutzung

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

9:45 bis 10:30 Uhr
Herausforderung VLAN-Planung
- Warum man immer mehr VLANs braucht
- Restriktionen der Komponenten
- Lösungsvarianten
- Ausblick auf neue Verfahren für eine langfristige Lösungen

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

10:30 bis 11:00 Uhr - Kaffeepause

11:00 bis 11:15 Uhr
Aufgabenstellung: ein hypothetisches Musterunternehmen

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

11:15 bis 12:45 Uhr
1. Herstellerrunde

12:45 bis 14:15 Uhr - Mittagspause

14:15 bis 15:45 Uhr
2. Herstellerrunde

15:45 bis 16:00 Uhr
Diskussionsrunde
- Welcher Ansatz ist der beste?
- Wo ist das Optimum?

16:00 Uhr - Ende der Veranstaltung

Auch die größten Puristen kommen an der Nutzung von VLANs zur Konfiguration Lokaler Netzwerke nicht vorbei. Aber VLANs bieten einen erheblichen Gestaltungspielraum und wer diesen nutzt, der wird schnell über das unvermeidbar Notwendige hinaus viele weitere VLANs anlegen. Sie können die Basis für Verkehrssteuerung sein, sie können als Sicherheits-Instrument eingesetzt werden oder als Basis für vereinfachtes Monitoring. So können auch mittelgroße Unternehmen schnell mit Tausenden und manchmal mit Zehntausenden von VLANs enden. Alleine diese Zahl macht auch klar, dass die Nutzung von VLANs auch zu betriebstechnischen Problemen führen kann. Kaum jemand wird in der Lage sein, ab einer bestimmten Anzahl von VLANs den Überblick zu behalten.

Also: wie viele VLANs braucht der Mensch in einem Lokalen Netzwerk? Die Antwort ist klar: so wenig wie nötig! Aber wie viel ist nötig und inwieweit unterscheiden sich die Sichtweisen der Hersteller zu diesem Thema? Ein gutes Beispiel ist die Diskussion um Voice- oder UC-VLANs. Bringen diese wirklich einen nachweisbaren Vorteil? Wird damit der angestrebte Schutz tatsächlich erreicht? Sind UC-VLANs nicht ein Widerspruch in sich selbst, wenn UC die IT-Integration anstrebt? Wieso sollte ich dann UC-Endgeräte von der IT mit einem VLAN trennen? Und was mache ich mit Soft-Clients?

Speziell auch im Umfeld virtualisierter Server ist das Thema spannend. Hier sind diverse Standards in der Entwicklung, um in den Servern genutzte VLANs konsistent zu halten mit der physikalischen Netzwerk-Konfiguration. Aber gerade in diesem Umfeld kann das Thema schnell komplex werden.

Es wird Zeit, dieses Thema intensiver zu diskutieren. Wir haben deshalb den Intensiv-Tag des ComConsult Netzwerk-Redesign Forums gewählt, um der Sache auf den Grund zu gehen. Frau Borowka-Gatzweiler und Dr. Moayeri werden in das Thema einführen und Standpunkt beziehen. Dann wird ein Unternehmens-Szenario vorgestellt und drei bis vier ausgewählte und eingeladene Hersteller stellen sich der Diskussion mit ihren Lösungsansätzen für das Szenario. Ziel ist, dabei auch die unterschiedlichen Sichtweisen der Hersteller zu diesem Thema transparent zu machen. Der Tag wird beendet mit einer offenen Diskussion des Themas.

Der Intensiv-Tag des ComConsult Netzwerk-Redesign Forums ist getrennt buchbar, wenn Sie nur an diesem Thema interessiert sind oder für den gesamten Kongress keine Zeit haben.

Der Intensiv-Tag des ComConsult Netzwerk-Redesign Forums 2012 ist getrennt buchbar, wenn Sie nur an diesem Thema interessiert sind oder für den gesamten Kongress keine Zeit haben.

Aktueller Kongress

ComConsult IPv6-Forum 2012

21.05. - 23.05.12 in Düsseldorf

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

IPv6 hinterlässt weiterhin gemischte Gefühle: auf der einen Seite kann sich kein Unternehmen der Einführung entziehen, auf der anderen Seite gibt es eine lange Liste von Problemen und Fragen. Vor seiner Einführung sind viele Fragen zu klären:

- Welche Komponenten, Server, Endgeräte aber auch Anwendungen sind betroffen?
- In welcher Reihenfolge sollen Komponenten angegangen werden?
- Welche konkreten Anforderungen gibt es an IPv6-fähige Infrastruktur-Komponenten wie Router und Firewalls, welche Facetten von IPv6-Fähigkeit kann es geben?
- Wie soll mit neuen Gerätetypen wie Tablets umgegangen werden, sollen alle neuen Geräteklassen immer sofort mit IPv6 starten?
- Wie können alte IPv4 Komponenten wie Drucker, Accesspoints, Scanner, Überwachungskameras usw. weiterhin eingebunden werden?
- In welchem Umfang müssen die aktuellen Sicherheitskonzepte überarbeitet werden?
- Welche Art von IPv6 Adresse macht am meisten Sinn? (Stichworte: Unique Local vs. Global, EUI-64 vs. Privacy Extensions)
- Und ganz wichtig, da hieran die meisten Projekte heute haken: wie verkaufe ich die Einführung unternehmensintern, so dass die notwendigen Ressourcen dafür freigegeben werden?

Auf jeden Fall bietet IPv6 auch erhebliche Chancen: Viele Netze leiden unter einem historisch gewachsenen IP-Design, das die Anforderungen heute nur unzureichend erfüllt. Der „Gutmütigkeit“ von IP ist es zuzuschreiben, dass es kaum zu Problemen kommt. Trotzdem gibt es vielfach Verbesserungsbedarf in Bereichen wie Strukturierung des Netzplanes, Übersichtlichkeit, Nachvollziehbarkeit und Dokumentation. Um den laufenden Betrieb nicht zu stören, wird bei IPv4 meist davon abgesehen, eigentlich dringend notwendige Änderungen durch zu führen.

IPv6 bietet nun die perfekte Gelegenheit für ein neues, sauberes IP-Design:

- Die Fehler der Vergangenheit können dieses Mal vermieden werden.
- Der Parallelbetrieb von IPv4 und IPv6 während der nächsten Jahre ermöglicht einen sanften Übergang vom alten zum neuen Design.
- Der vergrößerte Adressraum erlaubt einen langfristig skalierbaren Netzplan.
- Veraltete Routingprotokolle können bei IPv6 unberücksichtigt bleiben.

Aber: IPv6 ist anders als IPv4. Es hat andere Grundideen und ein IPv6-Design muss von Null begonnen werden. Dabei sind wichtige Design-Entscheidungen zu treffen.

Das ComConsult IPv6-Forum 2012 greift diese Aspekte strukturiert auf und zeigt den optimalen Weg nach IPv6. Top-Berater und versierte Anwender berichten von ihren Erfahrungen und stellen sich den Fragen der Teilnehmer.

Erfahren Sie,

- welche relevanten Änderungen IPv6 außer dem deutlich vergrößerten Adressraum mit bringt und wie sich diese auf das IP-Design und den Betrieb auswirken.
- wie es um die aktuelle und generelle Sicherheit von IPv6 bestellt ist. Ob die verfügbaren Produkte wie Firewalls und Router schon auf dem Stand den IPv4 erreicht haben und ob neue Gefahren durch IPv6 drohen.
- welche Verfahren für die Migration stehen zur Verfügung stehen, welche bei welchem Szenario Sinn machen, und wie eine „sanfte“ Migration beispielhaft aus sieht.
- wie er aktuelle Stand bei unternehmenskritischen Anwendungen, zentralen Netzwerkkomponetenten ist.
- welche Empfehlungen es aus der Praxis für den Betrieb von IPv6 Netzen gibt.

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.

Frühbucherphase bis zum 29.02.2012

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

ComConsult IPv6-Forum 2012

Ich buche den Kongress
ComConsult IPv6-Forum 2012
☐ vom 21.05. - 23.05.12 in Düsseldorf
zum Preis € 1.890,-- netto*
*gültig bis zum 29.02.2012 -
dann regulärer Preis € 2.090,-- netto

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 12

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

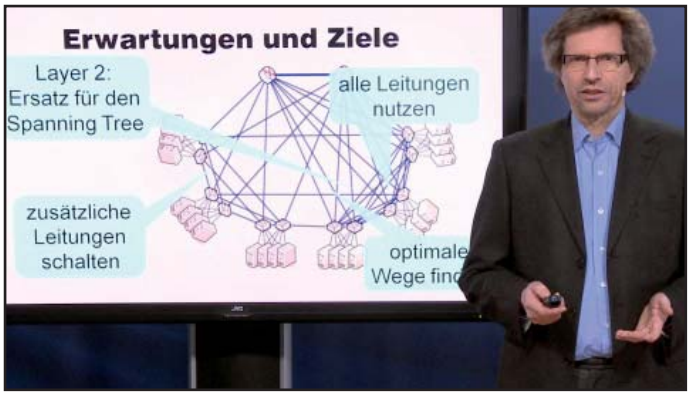
_____ Vorname	_____ Nachname
_____ Firma	_____ Telefon/Fax
_____ Straße	_____ PLZ,Ort
_____ eMail	_____ Unterschrift

ComConsult-Study.tv

Aktuelle Neuerscheinungen bei ComConsult-Study.tv

Themenbereich: Netzwerke

Seminar: TRILL kontra SPB: neue Netzwerk-Architekturen, aber wie?
Referent: **Dipl.-Math. Cornelius Höchel-Winter**
Zeit: 00:40:47 gesamt
Einzelpreis: 59,00 € netto Im Abo: kostenlos



Sternförmige Netzwerk-Architekturen im Rechenzentrum sind tot. Kurze und parallele Wege optimieren die Kommunikation zwischen Servern, Speicher und Applikationen. Zwei Standards kämpfen aktiv um die Vorherrschaft in diesem Bereich. TRILL von der IETF und Shortest Path Bridging von der IEEE. Hier geht es um mehr als nur um Switching-Standards, es geht um eine wesentliche Weichenstellung für das Netzwerk der Zukunft.

Themenbereich: Fotografie

Seminar: Monitore kalibrieren und profilieren
Referent: **Dipl.-Inform. Ulrike Häßler**
Zeit: 05:08:00
Einzelpreis: 59,00 € netto Im Abo: kostenlos

Die korrekte Farbwiedergabe von Monitoren ist für die Erstellung von Präsentationen, von Werbematerial oder für die Bearbeitung von Fotos von entscheidender Bedeutung. Aber häufig liegen Erwartungen und Ergebnisse weit auseinander. Woran liegt das?

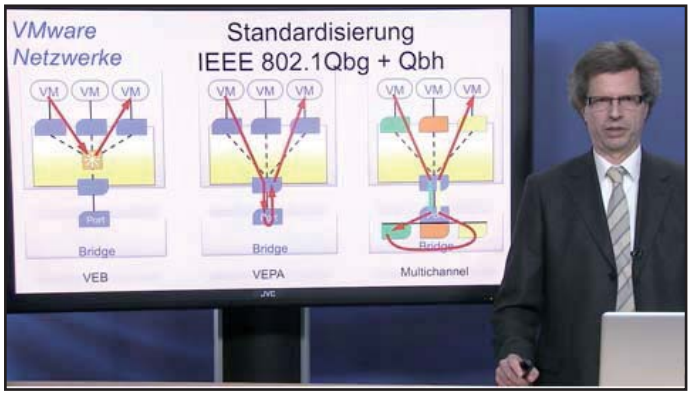
Themenbereich: Betrieb und Architekturen

Erfolgreich Präsentieren
Referent: **Lars Sudmann**
Zeit: erscheint in Kürze
Abo erforderlich

Erfolgreich und gut präsentieren können ist ein wesentlicher Baustein des beruflichen Erfolgs. Im Februar startet unsere neue Serie mit dem international anerkannten Präsentations-Experten Lars Sudmann

Themenbereich: Netzwerke

Seminar: Netzwerk-Integration virtueller Maschinen
Referent: **Dipl.-Math. Cornelius Höchel-Winter**
Zeit: erscheint im Februar
Abo erforderlich



Die richtige Anbindung virtueller Maschinen an Lokale Netzwerke ist ein Minenfeld. Neue Standards sind in Entwicklung, aber auch bestehende Lösungen erlauben sehr unterschiedliche Lösungen. Dabei werden Performance und Sicherheit wesentlich von der gewählten Lösung beeinflusst. Cornelius Hoechel-Winter stellt die Alternativen vor und bewertet sie.

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

Schwerpunktthema

Bring your own Device - Vorbote eines Umbruchs in der IT

Fortsetzung von Seite 1

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

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

Die „Consumerization“ stellt die IT dabei aber vor eine Vielzahl ungelöster Probleme. Standardisierung war und ist das grundlegende Credo der IT. Nur durch Standardisierung, so glaubte man, können die Kosten des IT-Betriebs gesenkt, sowie Sicherheit und Revisionsfähigkeit für Unternehmensdaten gewährleistet werden. Für weite Teile der IT-Landschaft ist dies auch nach wie vor gültig. Ohne Standardisierung sind Netz-Infrastrukturen und Rechenzentren schlicht nicht wirtschaftlich zu betreiben. Der Trend zu Consumerization ist somit auf die unmittelbare Nutzerschnittstelle, also Applikationen und Endgeräte beschränkt.

Im Bereich der Unternehmensanwendungen ist insbesondere ausschlaggebend, dass auf konsistenten Datenbeständen gearbeitet wird. Die Unternehmensdaten sollen eine einheitliche Basis des Geschäftsprozesses bilden. Wie das einzelne Nutzer-Frontend aussieht ist zweitrangig, solange es dem Anwender ein möglichst effizientes Arbeiten erlaubt. Effizientes Arbeiten ist aber genau dann möglich, wenn der Anwender die Bedienelemente versteht und zielgerichtet einzusetzen vermag. Und das möglichst intuitiv, ohne hohen Schulungsaufwand für die Unternehmen. Ob der Anwender seine Groupware mit einem Outlook-Client, einen Drittanbieter-Client oder über eine Weboberfläche abruft, ist für die Tätigkeit als solche irrelevant. Das Bedienkonzept von Applikationen ist aber – gerade im Bereich der mobilen Endgeräte – in höchstem Maße von der Endgeräte-Plattform abhängig. Hier gibt es bei der privaten Nutzung klare Präferenzen der Anwender, z.B. für Apple iOS oder Android-basierte Geräte. Geht man auf die Nutzerpräferenzen ein, so lassen sich Synergie-Effekte durch bessere Nutzerakzeptanz und Anwenderzufriedenheit, sowie geringeren Schulungs- und Betriebsaufwand nutzbar machen. Das ist der Kerngedanke von „Bring your own Device“ (BYOD).

2. Der Endgerätezoo

Consumerization führt dazu, dass die Mitarbeiter eine Vielzahl von Endgeräte-Plattformen in die Unternehmen tragen. Die Endgeräte-Hardware ist hochgradig individuell und wird von verschiedenen Herstellern wie Apple, HTC, Motorola, Nokia, RIM, Samsung oder Sony-Ericsson geliefert, um nur einige zu nennen. Die Betriebssysteme sind entweder herstellergebunden, wie Apple iOS und RIM Blackberry OS, oder für Hardware-Plattformen verschiedener Hersteller verfügbar, wie Android und Windows Phone 7. Während die Eigenschaften der Endgeräte-Hardware (Gewicht, Akkulaufzeit, Verarbeitungsqualität, Display, (Netz-) Schnittstellen, Bedienelemente) kaum Auswirkungen auf den Unternehmenseinsatz haben, ist das Betriebssystem sowohl in Hinblick auf Geschäftsapplikationen, Datensicherheit und Management der bestimmende Faktor.

Die heute relevanten Smartphone-Betriebssysteme sind Android, Apple iOS, und Blackberry OS. Während Apples abgeschottetes iOS mit dem starken Entwickler-Ökosystem und dem „Style-Factor“ den Boom der Smartphones befeuerte, setzte Google Android auf eine vergleichsweise offene Plattform und überrollte so den Consumer-Markt. Beide setzen damit RIM, dem ehemaligen Marktführer für geschäftstaugliche Smartphone-Lösungen, massiv unter Druck. Symbian hat seine Marktführerschaft aufgrund des verpassten Anschlusses an die Smartphone-Welt verloren.

Auch Windows Phone, der Nachfolger des im Geschäftsbereich erfolgreichen Windows Mobile, hat bislang keine nennenswerten Marktanteile gewinnen können. Es fristet momentan noch ein Nischendasein zusammen mit Betriebssystemen wie bada, dem von Samsung entwickelten, offenen Smartphone-Betriebssystem. Die Kooperation mit Nokia zeigt allerdings erste Erfolge. Die ersten Absatzzahlen der in Kooperation entwickelten Lumia-Endgeräte sind vielversprechend, und Marktforscher wie IDC und IHS isupply prophezeien eine Aufholjagd zu Android, Blackberry OS und iOS.

Die Aussagen der Experten, wie die Konkurrenten den Markt in den kommenden Jahren unter sich aufteilen werden, ge-

hen allerdings auseinander. Sicher ist nur, dass Android wohl die Marktführerschaft im Gesamtsegment ausbauen wird, man aber weiterhin mit mindestens vier verschiedenen Mobilplattformen rechnen muss. Hinzu kommt eine fast unüberschaubare Zahl von verschiedenen Releases, Versionsständen und herstellerspezifischen Adaptionen. All diese Plattformen bezüglich ihrer Sicherheitsaspekte im Blick zu behalten, ist eine Aufgabe, der kaum eine IT-Abteilung auf Dauer gewachsen sein dürfte.

Hinzu kommt, dass nicht nur Smartphones für eine BYOD-Strategie in Frage kommen. Der gesamte Client-Bereich dürfte in den kommenden Jahren zur Disposition stehen. Das Notebook hat den stationären PC in vielen Bereichen bereits verdrängt; niedriger Energiebedarf, geringe Geräuschentwicklung und vereinfachter Support bei gleichzeitig geringen Mehrkosten waren Haupttreiber für den Austausch stationärer Workstations durch mobile PCs. Auch die zunehmende Mobilität der Mitarbeiter hat diesen Trend befeuert. Doch der klassische, Windows-basierte Arbeitsplatz ist auf lange Sicht in Gefahr. Tablet-PCs bieten ein vollständig neues Bedienkonzept. Damit werden sie heute den Anforderungen einer vollwertigen Arbeitsplatzlösung noch nicht gerecht, sondern eigenen sich vor allem zum automatisierten Erfassen, Darstellen und Präsentieren von Informationen. Doch erste Geräte, wie z.B. das Transformer oder das Lapdock, erweitern Tablet bzw. Smartphone um eine Docking-Station mit integrierter Tastatur, womit die Leistungsfähigkeit der Nutzerschnittstelle nah an ein herkömmliches Notebook heranreicht. Andere Geräte, wie das voraussichtlich im Sommer verfügbare Padfone, kombinieren Smartphone und Tablet. Somit verschmelzen die Grenzen zwischen Smartphone, Tablet und Notebook. Spätestens mit Verfügbarkeit von standardisierter Business-Software, wie z.B. leistungsfähigen und kompatiblen Office-Anwendungen, wird die Grenze zwischen Office-PC und mobilem Endgerät fallen. Eine Integration in die Unternehmens-Infrastruktur zu realisieren und gleichzeitig die Vertraulichkeit der verarbeiteten Daten zu gewährleisten, ist schon bei einem standardisierten Client-Portfolio eine Herausforderung. Doch wie kann dies bei der Vielzahl von Endgeräten und Betriebssystemen in einem BYOD-Szenario erreicht werden?

3. Gefährdungen durch mobile Endgeräte und BYOD

BYOD ist zunächst mit dem grundsätzlichen Risiko des Verlusts von Vertraulichkeit und Integrität von Unternehmensdaten durch die Aufweichung der Abgrenzung von unternehmenseigener und fremder IT verbunden.

Als mobile Endgeräte sind dabei Smartphones und Tablets wie mobile PCs und mobile Datenträger einzustufen und entsprechenden Gefährdungen ausgesetzt. Hierzu zählen insbesondere die im Folgenden diskutierten Punkte:

Verlustrisiko (inklusive Diebstahl)
Mit dem Verlust eines Endgeräts besteht generell die Gefahr eines Verlusts von Unternehmensdaten (Dokumente, Kontakte, Passwörter, etc.) und des Zugriffs auf vertrauliche Informationen.

Transportwirt für Schadprogramme
Ein Smartphone oder Tablet ist in vielen Fällen ein Zwischenspeicher für per Internet, MMS oder SMS bezogene Daten, die manuell oder automatisch mit der Dateiablage in einem PC oder einer zentralen Dateiablage synchronisiert werden. Auf diese Weise lässt sich analog zu USB-Sticks Schadsoftware in das Unternehmensnetz einschleusen. Basis ist oft ein Web-Zugriff über den eine schadenstiftende Datei auf Smartphone oder Tablet heruntergeladen wurde.

Ziel für Schadprogramme
Smartphones und Tablets sind auch das direkte Ziel von schadenstiftender Software (Malware). Diese Gefahr darf nicht unterschätzt werden. Beispielsweise wird seit 2009 ein exponentielles Wachstum an Malware für Android festgestellt (siehe z.B. Malcious Mobile Threats, Report 2010/2011 von Juniper Networks). Die Konsequenzen eines Befalls mit Malware sind im Prinzip analog zu Windows-PCs. Beispiele sind:

- Zugriff auf vertrauliche Informationen, die auf dem Endgerät gespeichert sind (Dokumente, Passwörter, Kontakte, E-Mails, etc.)
- Gerät nicht länger nutzbar
- finanzieller Schaden durch missbräuchliche Nutzung von Mehrwertdiensten

Unberechtigter Zugriff auf Infrastruktur-Ressourcen
Über ein kompromittiertes mobiles Endgerät kann ein ggf. weitgehender Zugriff auf Unternehmensressourcen erfolgen, sofern der Zugang zur Infrastruktur nicht angemessen geschützt ist. Hier geht es nicht nur um Datendiebstahl. Als Szenario stelle man sich beispielsweise ein mit Malware verseuchtes Fremdgerät vor, das versucht alle erreichbaren Kommunikationsziele im Unternehmen zu infizieren.

Die Strategie zum Schutz vor den genannten Gefährdungen liegt auf der Hand:

- Härten der Systeme (sichere, zentrale Konfiguration, Virenschutz und Sandboxing)
- Absicherung des Zugriffs auf Infrastrukturressourcen

Welche Möglichkeiten und Grenzen hier für BYOD bestehen, wird in den folgenden Kapiteln erörtert.

4. Endgeräte-Management und User-owned Devices

Die Absicherung von unternehmenseigenen Endgeräteflotten wird in der Regel durch Mobile Device Management (MDM) Lösungen erzielt. Über diese Lösungen

kann der Endgeräte-Fuhrpark zentral gemanaged werden. Wesentliche Funktionen sind:

- Fernwartung
- Inventarisierung und Flottenmanagement
- Konfiguration
- Sicherheitsrichtlinien
- Softwareverteilung

Fernwartung, Inventarisierung und Flottenmanagement sind Funktionen, die in erster Linie den IT-Betrieb unterstützen sollen und für Administration und Support einer unternehmenseigenen Endgeräte-Flotte dringend benötigt werden. Fernkonfiguration und die Möglichkeit, Konfigurationsprofile, Softwarestände und Sicherheitsrichtlinien zu erzwingen sind wesentliche Funktionen, um eine Endgeräteplattform gegen Bedrohungen abzusichern. Es ist eine Vielzahl von Produkten am Markt verfügbar, die die für BYOD benötigte Multi-Plattform-Fähigkeit mitbringen.

Hersteller wie 7P, AirWatch, MobileIron, SAP/SyBase sind seit Jahren im internationalen Markt tätig. Hinzu kommen Anbieter, die mit Schwerpunkt im deutschsprachigen Markt aktiv sind, wie z.B. DIALOGS oder M-Way Solutions. Diese Anbieter setzen auf die Unterstützung von verschiedenen Endgeräte-Plattformen und sind somit prinzipiell für die Verwaltung von verschiedensten Endgeräten geeignet. Hinzu kommen zahlreiche Distributionspartner, wie z.B. RDS-Consulting, die modifizierte Varianten dieser Produkte anbieten. Mit Ubitexx wurde ein weiterer bekannter Spieler im deutschen Markt unlängst von RIM akquiriert. Ziel ist es vermutlich, die Ubitexx-Technologie in den Blackberry Enterprise Server zu integrieren. So könnte die bislang geschlossene Plattform zur Verwaltung von Blackberry Smartphones für iOS, Android und weitere mobile Betriebssysteme geöffnet werden. Damit wird auf den Trend zu diesen Plattformen reagiert und eine Öffnung hin zu BYOD vollzogen. Weitere Spieler, wie z.B. die von Gartner als führend im MDM-Markt eingeordnete Good Technology, verlassen den Pfad reinen Device Managements und setzen verstärkt auf die Bereitstellung speziell abgesicherter Enterprise-Applikationen.

Die oben genannten Lösungen unterscheiden sich teilweise stark in Funktionsumfang, Bedienbarkeit und Plattformunterstützung. Ein umfassender Vergleich würde Ziel und Rahmen dieses Artikels sprengen. Es ist aber festzuhalten, dass alle Lösungen je nach Endgeräte-Plattform Funktionsunterschiede aufweisen. Das liegt daran, dass einige Funktionen auf bestimmten Betriebssystemen aufgrund fehlender Schnittstellen nicht realisiert werden können. So wird z.B. durch einige Hersteller eine Softwareinstallation ohne Nutzerinteraktion (silent mode) für Windows Mobile implementiert, während dieselbe Funktion laut Herstellerangaben für Android und iOS technisch noch nicht möglich ist. Daher kann man für unterschiedliche Plattformen keine einheitlichen bzw. nur sehr eingeschränkte Sicherheitsmaßnahmen ergreifen. Dieser Umstand allein widerspricht schon einem Einsatz in Szenarien mit großer Endgeräte-Vielfalt.

Als alleinige Sicherheitsmaßnahme in einem BYOD-Szenario ist MDM im klassischen Sinn also nicht zielführend.

Hinzu kommt der Umstand, dass private Endgeräte per Definition der Kontrolle des Anwenders unterstehen. Wie aber soll der Anwender motiviert werden, sein Endgerät dem Regiment der Unternehmens-IT zu unterwerfen? Ist MDM überhaupt noch zeitgemäß oder kann in Zeiten von BYOD schlicht auf solche Ansätze verzichtet werden? Leider nicht, wie im Folgenden dargelegt wird.

5. Isolierte Daten versus versiegelte Endgeräte

Die klassischen MDM-Ansätze zielen in letzter Konsequenz auf die Härtung des Endgerätes gegen äußere Gefährdungen und Fehlbedienung ab, um Richtlinienkonformität für den Zugriff auf Unternehmensinfrastruktur zu erzwingen.

Die Folge ist, dass die Benutzbarkeit des Endgeräts leidet. Das ist mit BYOD, das auf eine gleichzeitige private und dienstliche Nutzung von Endgeräten hinausläuft, nicht vereinbar. Welcher Nutzer wird sein privates Endgerät schon für den Dienstgebrauch nutzen wollen, wenn dadurch die private Nutzung im unzumutbaren Maß eingeschränkt wird?

Das Ziel muss daher sein, die Sicherheit der Unternehmensdaten sicherzustellen, ohne die Privatnutzung in überbordendem Maß einzuschränken. Doch die private Nutzung widerspricht in vielerlei Hinsicht den üblichen Sicherheitsrichtlinien, die auf einem strikten White Listing von zulässigen Aktionen basieren.

Daher ist es sinnvoll, eine Trennung zwischen privater und dienstlicher Nutzung technisch zu erzwingen. Hierzu müssen die Applikationen abgesichert werden, in denen schützenswerte Daten verarbeitet werden. Mobile Applikationen können in verschiedener Art und Weise implementiert werden:

- Lokale Ausführung mit lokalem Datenbestand
- Lokale Ausführung mit zentralisiertem Datenbestand
- Zentralisierte Ausführung mit lokaler Darstellung

Die erste Variante ist in erster Linie für Anwendungen interessant, die nicht auf großen und stets aktuellen Datenbeständen arbeiten müssen. Ein Beispiel wären Hilfsprogramme und Office-Anwendungen. Doch selbst Office-Anwendungen müssen heute mit zentralen Speicherorten (File Server, Cloud Services) interoperabel sein. Auch Endgeräte-Virtualisierung im Sinne einer lokal ausgeführten virtuellen Maschine fällt in diese Kategorie. Die lokale Ausführung mit zentralisiertem Datenbestand ist insbesondere für Unternehmensanwendungen wie ERP/CRM und andere Datenbankanwendungen, sowie Groupware (Email, PIM) interessant. Die zentralisierte Ausführung mit lokaler Darstellung ist ein weites Feld. Hierunter fallen Web-basierte Applikationen, Server-based Computing und Endgeräte-Virtualisierung. Der größte Nachteil der ersten Variante ist, dass lokale Datenbestände auf dem Endgerät vorliegen, die sich zunächst der Kontrolle des Unternehmens entziehen. Außerdem besteht die erhöhte Gefahr, das Endgerät mit samt diesen Daten zu verlieren.

Dem wird durch zentrale Datenverarbeitung abgeholfen, die ein geschlossenes System mit definierten Nutzerschnittstellen darstellt. Die Daten verlassen die Grenzen des Unternehmens nicht bzw. nur insofern sie zur lokalen Darstellung benötigt werden. So erlaubt dieser Ansatz maximale Kontrolle über den Verbleib der Daten, was aus einer Sicherheitsperspektive eigentlich ideal wäre. Der große Nachteil von zentral bereitgestellten Applikationen ist jedoch, dass sie eine möglichst unterbrechungsfreie, performante Netzanbindung des Endgeräts voraussetzen. Das aber kann nach heutigem Stand für mobile Endgeräte nicht garantiert werden, so dass das Einsatzgebiet dieser Lösungen begrenzt ist.

Die zweite Variante (lokale Ausführung mit zentralisiertem Datenbestand) ist ein guter Kompromiss. Es werden nur die Daten im lokalen Cache vorgehalten, die für das Arbeiten mit der Anwendung notwendig sind. So verbleiben die Datenbestände unter der Kontrolle des Unternehmens, und nur Teile dieser Daten liegen lokal auf den Endgeräten vor. Die notwendige Rechenleistung für die lokale Ausführung al-

ler wesentlichen Business-Applikationen bieten die heutigen mobilen Endgeräte ohnehin. Zwar muss die Datenverbindung für ein zügiges Arbeiten ebenfalls performant sein, kurzzeitige Verbindungsunterbrechungen, wie sie typischerweise beim Roaming entstehen, sind aber unproblematisch.

Allen Ansätzen ist jedoch gemein, dass Daten - wenn auch eventuell nur ausschnittsweise - während der Verarbeitung bzw. Darstellung auf dem mobilen Endgerät vorliegen. Daher ist es wichtig, die lokalen Applikationsbestandteile besonders abzusichern. Hierzu müssen

- nicht-flüchtige Speicher,
- Arbeitsspeicher, und
- Schnittstellen

der Applikationen sauber isoliert sein.

Die Applikation muss Daten in einem privaten Bereich des internen Speichers oder auf der Speicherkarte verschlüsselt ablegen können. Um ein direktes Auslesen durch andere Applikationen während der Laufzeit zu verhindern, ist es ideal, wenn die Daten auch im Arbeitsspeicher verschlüsselt vorliegen. Erst bei Zugriff der Applikation auf ein bestimmtes Datum sollte diese durch die Applikation entschlüsselt werden. Bei einem Kontextwechsel, also dem Wechsel auf eine andere Applikation oder einen Hintergrundprozess, liegen diese Daten dann nicht mehr unverschlüsselt vor. Aus Performance-Gründen wird auf diese Maßnahme oft verzichtet und ein Zugriff auf den Kontext des Prozesses durch die Speicherverwaltung des Betriebssystems unterbunden. Weiterhin muss es dem Programmierer möglich sein, den Datenaustausch mit anderen Applikationen wirkungsvoll einzuschränken. Hierzu muss die Betriebssystem-API es ermöglichen, die Datenübergabe an andere Applikationen zu unterbinden, oder gezielt bestimmte Daten über eine definierte Schnittstelle freizugeben. Diese Mechanismen werden idealerweise durch das mobile Betriebssystem unterstützt, oder müssen durch die Anwendungsentwickler implementiert werden.

Das Ergebnis ist eine Isolation der Applikationen (siehe Abbildung 1), das sogenannte „Sandboxing“. Es schützt die Applikation vor Zugriffen durch andere Apps, verhindert aber andererseits auch unautorisierte Zugriffe der Applikation auf Systemressourcen.

Sandboxing wird von den am Markt verfügbaren Betriebssystemen in unterschiedlicher Ausprägung unterstützt.

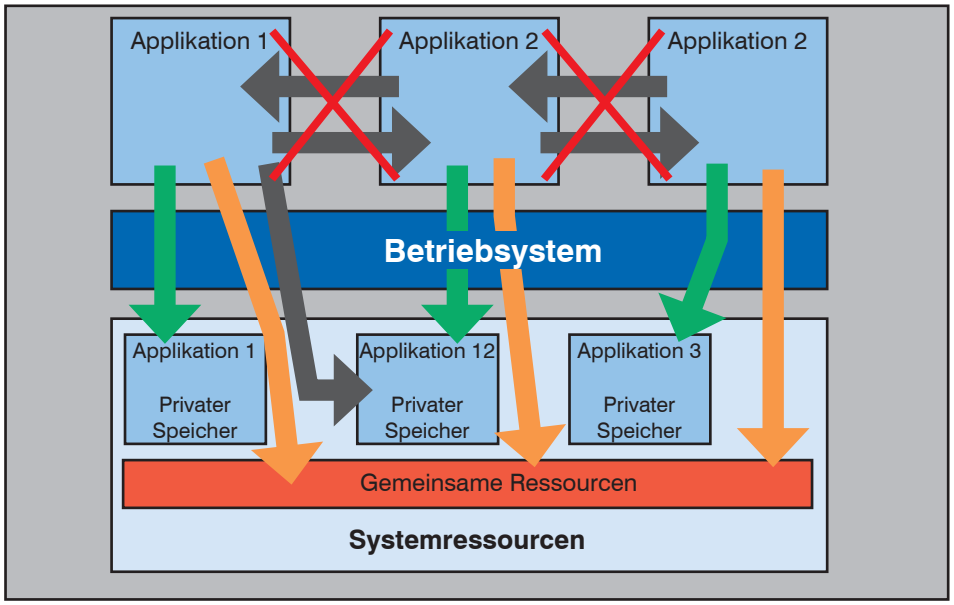


Abbildung 1: Sandboxing verhindert den unkontrollierten Zugriff auf Systemressourcen und andere Apps

Apple’s iOS ab Version 4 führt ein grundsätzliches Sandboxing aller Applikationen durch. Ein gemeinsames Dateisystem existiert nicht. Jede Applikation setzt auf einem eigenen, verschlüsselten Speicherbereich auf. Auf eine Verschlüsselung des Arbeitsspeicherinhaltes wird verzichtet und die Isolation durch die Prozessverwaltung des Betriebssystems realisiert. Jede Applikation läuft mit einer von fünf Berechtigungsstufen, anhand derer der Zugriff auf Systemressourcen eingeschränkt werden kann. Einige Systemressourcen können jedoch von jeder Applikation unkontrolliert genutzt werden. Darunter zählen auch potentiell kritische Ressourcen, wie der Zugriff auf Kalendereinträge, Kamera und Mikrofon.

Android verwendet zur Ausführung von Applikationen virtuelle Maschinen, wodurch eine grundlegende Trennung erzielt wird. Es kann, neben dem privaten Speicherbereich, lesend auf ein gemeinsames, unverschlüsseltes Dateisystem für Nutzerdaten zugegriffen werden. Der Arbeitsspeicherinhalt wird ebenfalls nicht verschlüsselt.

Auch unter Android sind Applikationen durch ein Rechtesystem voneinander getrennt. Anwendungen können aber immer eine Liste der installierten und ausgeführten Programme einsehen und andere Applikationen starten. Zudem können während der Installation weitere Rechte durch den Nutzer angefordert werden (z.B. Zugriff auf Ortinformationen), die der Anwender gewähren darf. So kann das Rechtesystem zur Kontrolle der Systemressourcen aufgeweicht werden.

Anhand dieser Beispiele wird deutlich, dass die Betriebssystem-eigenen Sandboxing-Mechanismen zwar geeignet sind, um Applikationen voneinander zu isolieren, nicht jedoch, um den Zugriff auf Systemressourcen zu unterbinden. Zudem können Exploits im Betriebssystem genutzt werden, um die Isolation der Anwendungsdaten zu durchbrechen. Eine wirkungsvolle Sandbox-Implementierung kann also nur durch den Anwendungsentwickler selbst vorgenommen werden.

Beispiele hierfür sind die Bridge-Application des Blackberry-Herstellers RIM und die Mobile-Lösung von Good Technology. RIM setzt die Bridge-Application ein, um die private und dienstliche Nutzung des Blackberry Playbook voneinander zu trennen. RIM geht von einer hinreichenden Härtung des Blackberry-Smartphones aus, welche durch restriktive BES-Policies herbeigeführt werden kann. Die Bridge Application stellt eine Verbindung via Bluetooth zum Smartphone her und stellt ausgewählte Applikationen in einer Sandbox auf dem Tablet bereit. Good Technology bietet einen Client für iOS und Android, der eine Sandbox für Unternehmensanwendungen wie E-Mail, PIM, File Server und Datenbankanwendungen implementiert. Neben dem nicht-flüchtigen Speicher des Clients wird auch der Arbeitsspeicher mit systemunabhängigen Credentials verschlüsselt. Bei Kontextwechsel wird so einem unautorisierten Zugriff auf den Speicher, z.B. über Betriebssystem-Exploits, vorgebeugt.

Beiden Lösungen ist aber eines gemeinsam: die Implementierung der Sandbox

auf Anwendungsebene erhöht zwar das Schutzlevel der Applikation und der verarbeiteten Daten. Sie kann jedoch keinen umfassenden Schutz vor dem Abgriff von Informationen direkt von den Nutzerinterfaces, z.B. Display und Tastatureingaben, garantieren. So könnten, durch die Ausnutzung von Betriebssystem-Exploits, weiterhin Daten via Screenshot oder Key Logger erfasst, sowie Nutzerdaten und Credentials ausgespäht werden.

Der Ausnutzung solcher Schwachstellen kann, bis zum Bekanntwerden und der Behebung durch den Hersteller, nur präventiv entgegen gewirkt werden. Es muss verhindert werden, dass die entsprechende Schadsoftware überhaupt auf das Endgerät gelangt. Geeignete Maßnahmen dafür sind:

- Erzwingen von Malware-Schutz für das Endgerät
- Überwachung und Einschränkung der Kommunikationsschnittstellen
- Steuerung der Endgerätekonfiguration
- Compliance Check bzw. Management von Software und Patches

Das sind aber genau die Fähigkeiten einer MDM-Lösung. Trotz Sandboxing der Applikation ist also eine Device Management Lösung weiterhin erforderlich, wenn sensible Daten verarbeitet werden. Grundlegende Mobile Device Management Fähigkeiten sind teilweise als Bestandteil von Sandboxing-Lösungen verfügbar und könnten optional eingesetzt werden. Wie bereits oben erläutert, widerspricht die restriktive Endgerätekontrolle aber dem Grundgedanken von BYOD.

Es gibt nun vier Möglichkeiten, mit diesem Sachverhalt umzugehen:

1. Man sieht von einer BYOD-Strategie vollständig ab und nutzt weiterhin einen firmeneigenen, voll gemanagten Endgeräte-Pool.

2. Man setzt einen firmeneignen, voll gemanagten Endgeräte-Pool um, wobei dem Anwender die Wahl zwischen verschiedenen, zugelassenen Endgeräten gegeben und eine private Mitnutzung gestattet wird.

3. Man setzt BYOD ausschließlich mit einer Sandboxing-Lösung ohne MDM-Funktionalität um und ignoriert das Restrisiko, das von Key-Loggern und anderer Malware ausgeht. So kann aber eigentlich nur verfahren werden, wenn die verarbeiteten Daten keinen erhöhten Schutzbedarf hinsichtlich der Vertraulichkeit haben.

4. Man setzt BYOD um und differenziert in mindestens zwei Nutzergruppen: Diejenigen Nutzer, die einem Management und einer Compliance-Überprüfung ihrer privaten Endgeräte widersprechen, erhalten nur Zugriff auf unkritische Daten und einen eingeschränkten Handlungsspielraum innerhalb der Unternehmensapplikation. Nutzer, die eine verstärkte Kontrolle des Endgeräts zulassen, erhalten mehr Rechte und Zugriff auf Informationen mit höherer Sicherheitseinstufung. (siehe Abbildung 2)

Insbesondere die Varianten 2 und 4 sind interessante Wege, um die Vorteile von BYOD bei gleichzeitig hohem Sicherheitsniveau zu nutzen. Variante 2 ist kein „echtes“ BYOD. Sie bietet dem Anwender aber die Möglichkeit, seine Wunschplattform zu nutzen, ohne ein weiteres Endgerät für den Privatgebrauch zu benötigen. Variante 4 ist BYOD im eigentlichen Sinne, bindet aber den Anwender in Sicherheitsfragen ein und schafft so ein erhöhtes Problembewusstsein. Bei Zustimmung zur Endgerätekontrolle profitieren diese Nutzer nicht nur durch den erweiterten Funktionsumfang, sondern auch vom erhöhten Sicherheitslevel ihres Endgerätes beim privaten Gebrauch, also z.B. der Möglichkeit Privatdaten bei Verlust des Endgerätes zu löschen. Während für Variante 1 ein herkömmliches MDM ausreicht, eignet sich zur Umsetzung der Varianten 2 und 4 besonders eine Mobile-Lösung, die Sandboxing von Enterprise-Applikationen mit grundlegendem Mobile Device Management und einer Gruppenverwaltung kombiniert.

6. Herausforderung Netzzugang

Für BYOD ist die grundsätzliche Entscheidung zu treffen, ob neben dem Zugang über das Mobilfunknetz (UMTS und künftig vermehrt LTE) auch die Verwendung des WLAN an einem Unternehmensstandort erlaubt wird. Dies ist immer dann interessant, wenn an einem Standort nur eine unzureichende Mobilfunkversorgung besteht.

Wenn BYOD auch auf Notebooks ausgedehnt (oder eine – aktuell noch seltene – Docking Station für ein Tablet mit Ethernet-Anschluss unterstützt) werden soll, muss zusätzlich der kabelbasierte Netzzugang betrachtet werden. In diesem Fall ist die zwingende Konsequenz eine mandan-

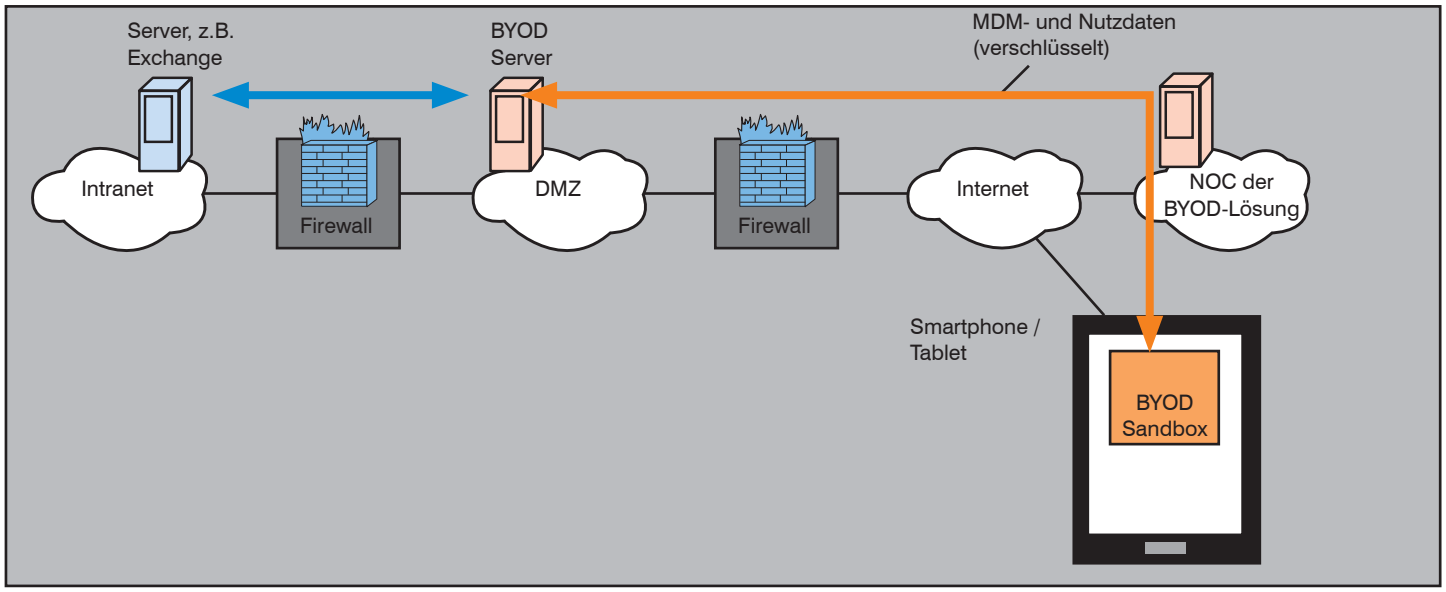


Abbildung 2: Sandbox-basierte BYOD-Lösung mit MDM

tenfähige LAN-Infrastruktur in Verbindung mit einer Netzugangskontrolle (Network Access Control, NAC), denn es müssen zumindest zwei Gruppen im Netz getrennt werden:

- Fremdgeräte, die nach einem Anschluss an einen Netzwerk-Port einen strikt eingeschränkten Zugang (z.B. über SSL-VPN und Terminal Server bzw. VDI) erhalten

- Eigene Geräte, die nach einer entsprechenden Authentisierung z.B. mit IEEE 802.1X den gewünschten (ggf. uneingeschränkten) Netzzugang erhalten

Während man im WLAN eine Mandantenfähigkeit durch das Controller-basierte WLAN-Design mit Leichtigkeit implementieren kann (Abbildung 3), sind im kabelbasierten LAN im Campus-Bereich spezifische, durchaus komplexe Techniken erforderlich.

Eine typische Vorgehensweise für das kabelbasierte LAN ist die Unterteilung des Netzes in einen internen und in einen externen (unsicheren) Bereich und die Nutzung von Virtual Routing and Forwarding (VRF) zur logischen Trennung beider Gruppen auf Layer 3. Die Zuordnung eines Geräts zum internen oder externen Bereich kann dann mit den Mitteln einer Netzugangskontrolle (IEEE 802.1X) erfolgen. (siehe Abbildung 4)

Aber auch im WLAN sind für BYOD noch weitere Punkte zu beachten. Zunächst ist zu klären, ob und wie eine Authentisierung und Verschlüsselung der WLAN-Kommunikation auch für BYOD-Geräte erfolgen muss. Hier wird oft argumentiert, dass es sich ja um Fremdgeräte handelt, für deren Absicherung der Kommunikation (ähnlich wie bei WLAN Hotspots) der jeweilige Nutzer und nicht der WLAN-Anbieter verantwortlich ist. Für BYOD mit Zugang über das Campus-WLAN muss hier genauer hingeschaut werden.

Wenn für ein BYOD-Gerät ein Internet-Zugang über das Campus-WLAN gestattet werden soll, sind zusätzliche Sicherheitsmechanismen erforderlich, die zumindest eine Authentisierung und Berechtigung der Internet-Nutzung überprüfen. Dies kann im einfachsten Fall wie in öffentlichen Hotspots über ein Captive Portal erfolgten. Der Nutzer startet hierzu seinen Browser, wird auf eine Login Web-Seite umgeleitet und gibt dort Nutzername und Passwort ein. Nach erfolgreicher Prüfung wird der Internetzugang dann hergestellt, über den dann wie über UMTS auf gesicherte Weise auf die IT-Infrastruktur zugegriffen werden kann. Dies setzt natürlich

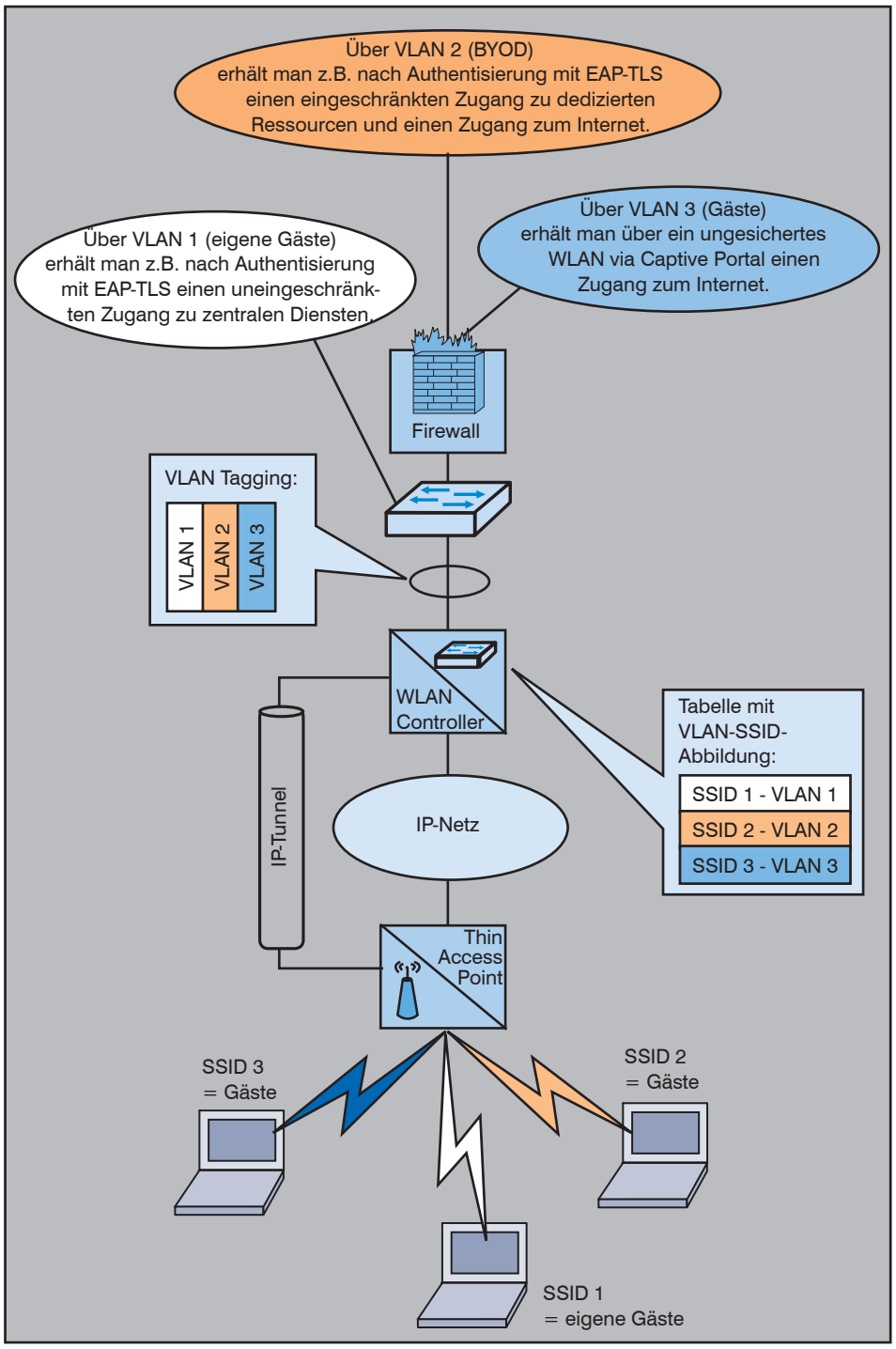


Abbildung 3: Beispiel für BYOD im WLAN

eine Kontoverwaltung für die BYOD-Nutzer voraus. Nachteilig ist hier, dass die WLAN-Kommunikation des BYOD-Geräts nicht auf Layer 2 im WLAN verschlüsselt wird und das Endgerät grundsätzlich über das WLAN so deutlich angreifbarer ist.

Grundsätzlich kann aber auch über eine MDM-basierte BYOD-Lösung ein deutlich besseres Sicherheitsniveau geschaffen werden, das zudem für den Nutzer bequemer ist. Über das MDM kann auf das Endgerät beispielsweise ein Zertifikat ausgerollt werden, über das sich das Gerät dann am WLAN auf eine sichere Weise mit IEEE 802.1X und EAP-TLS authentisiert. Nach erfolgreicher Authentisierung kann dann AES-basiert mit CCMP die WLAN-Kommunikation nach dem Stand der Technik verschlüsselt werden. Zumindest kann über das MDM ein Pre-Shared-Key bzw. das zugehörige

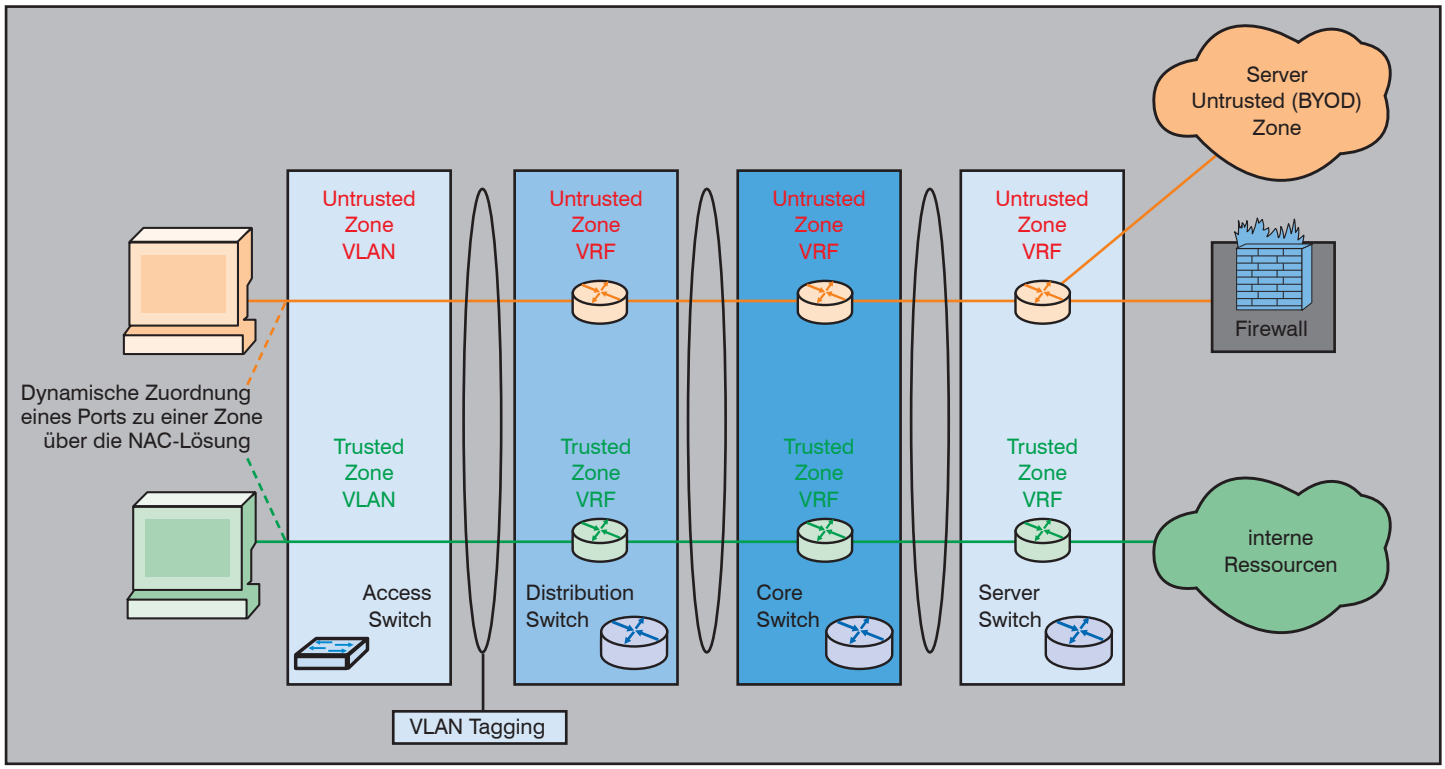


Abbildung 4: Illustration der Komplexität von BYOD im kabelbasierten LAN

Passwort verteilt werden, was bei hinreichender Komplexität und regelmäßiger Änderung sicherheitstechnisch noch vertretbar sein kann.

7. Fazit

Es steht außer Frage, dass mit der zunehmenden IT Consumerization ein tragfähiges Konzept für BYOD gefunden werden muss. Schon heute werden privat genutzte Endgeräte, wie z.B. Apple iPhone und iPad, im Widerspruch zu existierenden Sicherheitsrichtlinien für dienstliche Zwecke eingesetzt. Doch damit nicht genug: BYOD beschränkt sich nicht auf Smartphones und Tablets. Mit dem Verschmelzen von Notebook, Tablet und Telefon sowie einer zunehmenden Mobilisierung der Mitarbeiterschaft, muss das herkömmliche Konzept vertrauenswürdiger Clients generell in Frage gestellt werden. Dieser Tatsache können sich die Sicherheitsverantwortlichen in den Unternehmen nicht verschließen und sollten versuchen, das Beste aus dieser Situation zu machen.

Klar ist, dass einem nicht vertrauenswürdigen Endgerät kein direkter und unkontrollierter Zugriff auf die IT-Infrastruktur gestattet werden darf. Durch eine entsprechende Zonierung und ein wirksames Zugangskontrollsystem müssen Datenbestände und Dienste vor unbefugtem Zugriff geschützt werden. Die Autorisierung darf aber nicht mehr das Endgerät insgesamt erhalten, sondern nur noch eine Auswahl von Applikationen, welche sich mit Nutzer-Credentials authentisieren. Ein solches Zugriffsmodell ist nicht nur für die Bereitstellung in unternehmensinternen Rechenzentren, sondern auch für die Verwendung von Cloud Services geeignet. Die lokalen Applikationen müssen durch Sandbox- bzw. Virtualisierungs-Verfahren vom privat genutzten Teil des Endgeräts isoliert werden, und eine gesicherte Verbindung zur Unternehmensinfrastruktur aufbauen. Um Attacken gegen die Sicherheitsmechanismen von Applikation und Betriebssystem zu erschweren, ist ein grundlegendes MDM trotzdem weiterhin erforderlich.

Ob Applikation, Sandboxing-Technik und MDM-Lösung dabei aus einer Hand kommen müssen, sei einmal dahin gestellt. Wichtig ist es jedoch, dass in den Bereichen der Applikationsschnittstellen, der Sicherheitsmechanismen und der Management-Fähigkeiten mobiler Plattformen endlich tragfähige Standards geschaffen werden. Nur so kann die Interoperabilität mit Infrastrukturen anderer Unternehmen (Stichwort: Gastzugang) und die Transparenz des tatsächlich implementierten Schutzniveaus hergestellt werden. Sobald Lösungen, die diesen Anforderungen entsprechen, sowohl für mobile Plattformen als auch für den „klassischen“ Client verfügbar sind, steht der Vision von der überall verfügbaren IT aus der Steckdose nichts mehr im Wege.

8. Abkürzungen

AES	Advanced Encryption Standard
API	Application Programming Interface
BES	BlackBerry Enterprise Server
BYOD	Bring Your Own Device
CCMP	Counter Mode with Cipher Block Chaining Message
CRM	Customer-Relationship-Management
EAP	Extensible Authentication Protocol
ERP	Enterprise Resource Planning
IEEE	Institute of Electrical and Electronics Engineers
LAN	Local Area Network
LTE	Long Term Evolution
MDM	Mobile Device Management
MMS	Multimedia Messaging Service
NOC	Network Operation Center
OS	Operating System
PIM	Personal Information Manager
RIM	Research In Motion
SMS	Short Message Service
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
VDI	Virtual Desktop Infrastructure
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
WLAN	Wireless Local Area Network

Neues Seminar

Anwendungs-Virtualisierung für Android, iPad & Co

Die ComConsult Akademie veranstaltet am 29.03.12 erstmalig ihr neues Seminar „Anwendungs-Virtualisierung für Android, iPad & Co“ in Bonn.

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

Daraus resultiert eine Reihe von Fragen: Welche mobilen Geräte werden das größte Wachstum in den Unternehmen haben? Welche Applikationen werden hier speziell angesprochen? Warum werden hierdurch Cloud-Dienste in die Unternehmen tragen? Wie können die damit verbundenen Sicherheitsprobleme gelöst werden?

Die Frage nach den unternehmenskritischen Applikationen und der damit verbundenen Sicherheitsproblematik drängt die Frage nach Cloud-Diensten im eignen RZ förmlich auf. Denn niemand will ernsthafterweise seine Kunden- und Unternehmensdaten in einer öffentlichen Cloud wissen.

Zu hoch ist hier das Risiko des Datenverlustes oder der nicht Verfügbarkeit.

Gerade im Bereich Sicherheit entstehen aber signifikante Risiken. Mobile Geräte können verloren gehen oder gestohlen werden. Viele Anbieter bieten eine Verschlüsselung der lokal gespeicherten Daten, ein Remote-Wipe und die Konfiguration einer Reihe von einfachen Policies, sowie konfigurierbare VPN-Lösungen und realisieren damit eine einfache Benutzerverwaltung, aber das wird vielen Unternehmen nicht ausreichen.

Auch werden nicht alle Anwendungen über das aktuell diskutierte „Allheilmittel“ HTML5 bzw. mittels Webtechnologien den Usern zur Verfügung gestellt werden können.

Hier schlägt nun die Stunde der Virtualisierung und der Cloud-Dienste im RZ.

Diese Technologie, die mit Hilfe von virtuellen Umgebungen dem Anwender eine ihm vertraute Arbeitsumgebung, unabhängig von seinem Standort oder dem genutzten Client, zur Verfügung stellt, ist noch relativ jung was ihre Verbreitung anbelangt.

Bei der Anwendungs-Virtualisierung wird die Arbeitsumgebung für eine Applikation virtuell nachgebildet. Dadurch wird die Softwareverteilung für alle betroffenen Endgeräte vereinfacht. Die Client Software wird dabei auf einem zentralen Server vorgehalten. Hierzu sind zunächst Softwarepakete zu generieren. Diese Pakete werden den Benutzern bei Bedarf zur Verfügung gestellt. Der Anwender kann dann über einen Link auf seinem Endgerät (SmartPhone, Tablet- oder Desktop- PC) die virtuellen Anwendungen von einem Server abrufen.

Führende Anbieter sind, wie im Bereich der Server- oder Desktop-Virtualisierung, die Firmen VMware, Citrix und Microsoft. Die zur Verfügung stehenden Lösungen sind jedoch sehr unterschiedlich. Lösungsansätze für anwendungsspezifischen, virtuellen Umgebung werden umgesetzt von Produkten wie: Microsoft App-V, VMware ThinApp, oder Citrix XenApp

Ziele

- die Vor- und Nachteile der genannten Produkte sowie ihre Kompatibilität mit den verschiedenen mobilen Endgeräten aufzuzeigen,
- einen Überblick zur Leistungsfähigkeit zu geben
- sowie die eingangs gestellten Fragen zu beantworten.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Anwendungs-Virtualisierung für Android, iPad & Co

Ich buche das Seminar
Anwendungs-Virtualisierung für Android, iPad & Co

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

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

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

Standpunkt Sicherheit

Sicherheitsrisiko Firewall

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.

Firewalls haben sich in Netzwerken als Sicherheitsinstrument ausgehend vom Perimeter in der gesamten internen IT-Infrastruktur ausgebreitet. Wir finden inzwischen Firewalls zur Kontrolle der Kommunikation an WAN-Verbindungen, Partnerfirmenanbindungen, im RZ, im Server-Bereich und im Campus LAN für den Aufbau von (nicht selten mehrstufigen) Sicherheitszonen. Firewalls werden auch direkt vor zu schützende Geräte gesetzt (Device-attached Firewall), wie es beispielsweise im Industriebereich für den Schutz kritischer Produktionsanlagen gang und gäbe ist.

Woher kommt dann der offenkundige Reflex zur Firewall? Es beginnt meist mit der Feststellung, dass gewisse Systeme (SAP, UC, Datenbanken, etc.) einen erhöhten Schutzbedarf aufweisen. Für den Sicherheitsbeauftragten ist dann oft sofort klar: Diese Systeme müssen durch eine Firewall geschützt werden.

Die Firewall-Inflation erweckt auch den Eindruck, dass Firewalls offensichtlich in vielen Bereichen der IT eine sinnvolle Schutzfunktion haben und bei Bedarf als eine Art Standardkomponente sehr flexibel, en passant und mit einem vertretbaren Aufwand integriert und betrieben werden können.

Die Realität sieht leider anders aus! In verschiedensten Projekten haben wir immer wieder folgende Erfahrungen gemacht:

- Es gibt Firewalls mit 500 bis 1000 Regeln, und diese Firewalls sind praktisch nicht mehr verwaltbar. Wer kann die Auswirkung bei einem Change noch bewerten? Also gibt es höchstens noch neue Regeln aber kein Aufräumen im bestehenden Spagetti-Code.

- Firewalls werden oft bewusst auf „Durchzug“ gestellt, da z.B. der Quell-IP-Range oder der Ziel-Port-Range für Zugriffe nicht mehr genau genug festgelegt werden kann (was beispielsweise praktisch immer der Fall ist, wenn VoIP und UC sowie Client- und Server-Verkehr in Verteilten Systemen z.B. der Bauart Microsoft Windows zu filtern ist).

Wir können hieraus keineswegs ableiten, dass Firewalls sprich Filtermechanismen überflüssig sind. Die Firewalls sind ja schließlich aufgrund konkreter Sicherheitsanforderungen installiert worden. Wir müssen eher schließen, dass wir offensichtlich ein Werkzeug über Gebühr oder falsch eingesetzt haben. Woran fehlt es also?

Eine erste Antwort wäre: Wir brauchen mehr Anwendungsintelligenz und nutzerbezogene Regeln in Firewalls. Das ist genauso richtig wie falsch.

Es ist richtig, weil eine Firewall ansonsten viele Kommunikationsformen nicht mehr sinnvoll filtern kann.

Es ist falsch, denn die Firewall wird so immer unberechenbarer. Je mehr Intelligenz in der Firewall steckt, desto mehr Rechenleistung ist erforderlich und desto weniger ist das Antwortzeitverhalten der Firewall voraussagbar. Wir erleben immer wieder einzelne Anwendungen, die äußerst empfindlich gegenüber dem zusätzlichen Delay durch eine Firewall sind. Außerdem kann die Entscheidung, warum ein Paket verworfen wird, bei einer anwendungs-intelligenten Firewall vielleicht noch der entsprechende Software-Entwickler nachvollziehen, für den Administrator gibt es hierzu oft keine Chance mehr. In Konsequenz werden Firewalls immer mehr zu einer Black Box! Eine Sicherheitskomponente, deren Fehlverhalten im schlimmsten Fall die IT lahmlegen kann, muss aber zwingend einschätzbar sein. Eine Black Box ist hier nicht akzeptabel.

Können wir diesem Dilemma entkommen? Nein, denn dies würde eine Offenheit der Firewall-Hersteller erfordern, die wir wahrscheinlich nie bekommen werden.

Wir müssen also anders vorgehen. Zunächst darf die Entscheidung, ob gewisse interne Netzbereiche mit einer Firewall abzusichern sind, nicht pauschal bzw. reflexartig getroffen werden. Wir könnten außerdem Sicherheitsfunktionen wieder auf mehr Komponenten verteilen, um die Black Boxes kleiner und damit einschätzbarer zu halten und um die Sicherheitsfunktionen zielgerichtet einsetzen zu können. Hierzu kann insbesondere eine klare Trennung zwischen

- grober Verkehrsregelung (was eine klassische Stateful Inspection Firewall sehr gut übernehmen kann),
- nutzer- und anwendungsbezogener Berechtigung (hier sind Next Generation Firewalls im Vorteil) sowie der
- Filterung von Malware (d.h. das klassische Intrusion Prevention System - IPS)

dienen. Nur das hat seinen Preis.

Zweitthema

Funktionsreichtum kontra Vereinfachung

Fortsetzung von Seite 1

Dr. Behrooz Moayeri ist bei der ComConsult Beratung und Planung GmbH als Mitglied der Geschäftsleitung tätig. Er hat in den letzten beiden Jahrzehnten viele Unternehmen zur IT-Infrastruktur beraten.

Auch das Netz unterliegt diesem Gesetz und weist im Laufe seines historischen Wachstums eine steigende Entropie, sprich eine steigende Komplexität auf. Wenn man auch noch vom Beginn an eine komplexe Netzstruktur plant, läuft man Gefahr, dass das Gebilde schon bald nach der Inbetriebnahme unbeherrschbar wird.

Aber die Nachfrage nach mehr Funktionen ist ja nicht unbegründet. Nehmen wir das Beispiel LAN Security. In den letzten Jahren haben wir im Auftrag unserer Kunden immer mehr Lokale Netze mit der Funktion Network Access Control (NAC) konzipiert, getestet und dem Betrieb übergeben. Den meisten NAC-Projekten sind die Ziele gemeinsam, erstens das LAN vor unbefugten Zugriffen zu schützen und zweitens bereits beim physikalischen Anschluss eines Gerätes an das LAN das Gerät automatisch einer von mehreren Benutzergruppen zuzuordnen, die sich hinsichtlich ihres Schutzbedarfs wesentlich unterscheiden. Dies erfolgt in Form einer dynamischen Zuordnung zu einem Virtual Local Area Network (VLAN).

Beide Ziele lassen sich vom realen Bedarf der Unternehmen ableiten. Vor dem Hintergrund der zunehmenden Sicherheitsvorfälle passt ein offenes, ungeschütztes LAN nicht mehr zur heutigen Zeit. Hinzu kommt, dass in Räumlichkeiten vieler Unternehmen immer mehr Geräte vernetzt werden müssen, die nicht einer einheitlichen administrativen Hoheit und damit einheitlichen Sicherheitsrichtlinien unterliegen. NAC ist die Voraussetzung für den Aufbau eines mandantenfähigen LAN, das logisch in separate Segmente für die Aufnahme von Geräten mit unterschiedlicher Security-Einstufung aufgeteilt wird.

Aber NAC erhöht die Komplexität des Netzbetriebs. Unsere NAC-Erfahrungen der letzten Jahre belegen die Warnung, dass die Komplexität von NAC nicht unterschätzt werden darf. Mit NAC tritt eine Wechselwirkung zwischen Endgeräten und ihren Betriebssystemen einerseits und den LAN-Komponenten andererseits in Kraft, die uns bis vor wenigen Jahren unbekannt war. Mit NAC bürden wir dem LAN-Betrieb neue Aufgaben auf. Die Fehlersuche wird komplexer, die Abhängigkeiten von Funktionen und Mechanismen außerhalb des Einflusses von LAN-Betreibern (zum Beispiel Verzeichnisdiensten, vgl. Abbildung 1) größer.

Ein anderes Beispiel ist die Quality of Service (QoS). Wir erleben nunmehr das zweite Jahrzehnt der Diskussion über das Für und Wider von QoS in Lokalen Netzen. Vor allem die Einführung von Voice over Internet Protocol (VoIP) hat diese Funktion beflügelt. VoIP-Hersteller zwangen viele LAN-Betreiber mit ultimativen Forderungen nach QoS zu Einstellungen auf LAN Switches, deren Sinnfälligkeit immer wieder bezweifelt wird. Die zunehmende Nutzung von Video, der verstärkte Einsatz von Unified Communications (UC) auf Geräten, die nicht nur der Audio- und Videoübertragung, sondern vielmehr als Basis diverser Anwendungen dienen, die vielen Probleme gerade durch die Einführung von QoS und die explosionsartige Vervielfachung der verfügbaren Übertragungskapazität in Lokalen Netzen haben immer wieder die Frage aufgeworfen, ob QoS-Konzepte, die vor über zehn Jahren für die damalige Generation von VoIP-Endgeräten erstellt wurden, noch zeitgemäß sind.

Auch so alt wie IP-Telefonie ist die Diskussion über die Energiefunktionen von LAN-Switches. Um den Kunden die Hemmschwelle bei der Einführung von VoIP zu nehmen, sollten IP-Telefone wie seit über

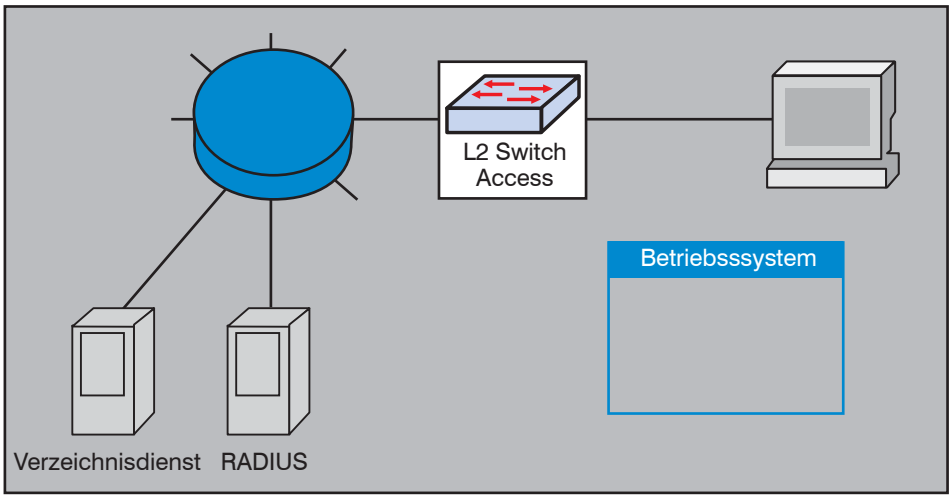


Abbildung 1: Einflussfaktoren bei NAC

hundert Jahren bei klassischen Telefonen der Fall „vom Netz gespeist“, d. h. von den Switches mit elektrischer Energie versorgt werden. Dass diese Forderung viele Detailprobleme verursacht, von der Erkennung des Leistungsbedarfs der Endgeräte durch den Switch bis zur Überlegung, auf welche Gesamtleistung von angeschlossenen Endgeräten ein Switch ausgelegt sein sollte, ist angesichts von über zehn Jahren Erfahrung mit Power over Ethernet (PoE) unbestritten. Qualvoller wurde die Wahl zwischen verschiedenen PoE-Optionen dadurch, dass mittlerweile nicht nur VoIP-Endgeräte, sondern auch Wireless Access Points mit PoE versorgt werden und weitere Gerätetypen wie Docking Stations als Kandidaten für PoE im Gespräch sind.

Einige Hersteller sind auf die Idee gekommen, LAN-Switches nicht nur für die Versorgung von Endgeräten mit Energie, sondern darüber hinaus auch für die Implementierung von Funktionen des Energiemanagements zu nutzen, die eine breite Palette von der reinen Überwachung und dem Reporting des Energieverbrauchs bis hin zur Steuerung von Endgeräten und deren Energieaufnahme reichen. Die immer wieder aufgegriffene Thematik der „Green IT“ leistet solchen Konzepten Vorschub.

Ganze Seiten voll kann man über Pro und Kontra VLANs schreiben. VLANs können zur Trennung von Benutzergruppen, für Netzmanagement, zur Isolierung bestimmter Gerätetypen wie Telefone, Gebäudemanagementeinrichtungen, Wireless Access Points etc. eingesetzt werden. Mit VLANs ist aus einem Layer-2-Switch schnell eine Reihe von logisch getrennten Switch-Instanzen gemacht (siehe Abbildung 2). Aber auch hier stellt sich die Frage: Ist ein VLAN-Flickenteppich noch beherrschbar? Wird durch die exzessive VLAN-Nutzung die Fehlersuche nicht komplexer, die Gefahr von Fehlfunktionen nicht größer und damit die Verfügbarkeit des Netzes nicht reduziert? Kommt die Netzdokumentation noch mit, wenn die VLAN-Konfiguration jedes Switches anders aussieht als die jedes anderen Switches?

Während über NAC, QoS, PoE und VLANs schon seit Jahren kontrovers gesprochen wird, hat der Wandel der Rechenzentrumsstrukturen in den letzten zwei bis drei Jahren neue Diskussionen darüber aufkommen lassen, was von neuen Funktionen für RZ-Netze zu halten ist, welche von den aktuellen Produkten angeboten werden: Link State Bridging, prioritätsgesteuerte Flusskontrolle (Priority-Based Flow Control, PFC), Enhanced Transmission Selection (ETS). Diese Funktionen werden oft mit der Forderung begründet, Speicherverkehr über Ethernet zu leiten. Speichersysteme kommunizieren aber teilweise seit Jahren über Ethernet, und zwar ohne dass es Data Center Bridging (DCB), also solche Funktionen wie PFC und ETS gibt. Warum müssen RZ-LANs neu erfunden werden, wenn es auch anders geht?

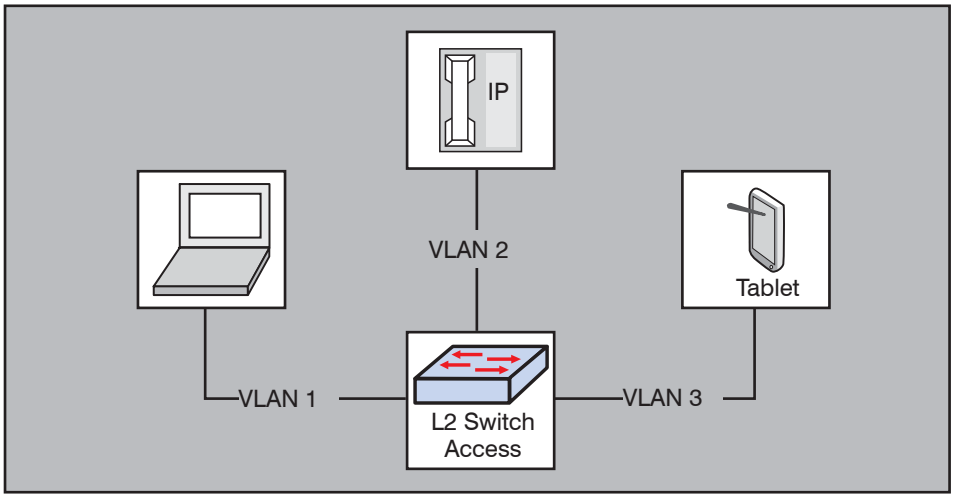


Abbildung 2: Einsatz von VLANs für logische Segmentierung

Mindestens seit drei Jahren wird im Markt sehr intensiv über künftige Layer-2-Verfahren gesprochen. Noch bevor sich die Branche auf einen Standort für Link State Bridging einigen konnte, haben mehr oder weniger alle Hersteller Mechanismen für Multi-Chassis Link Aggregation (MC-LAG) in ihren Produkten implementiert. Proprietäre Varianten von Link State Bridging sind mittlerweile auch verfügbar. Da die meisten Layer-2-Netze ohnehin auf Spanning Tree und Rapid Spanning Tree basieren und höhere Anforderungen an die Geschwindigkeit der Umschaltung zunehmend mit MC-LAG erfüllt werden, stellt sich die Frage, wer noch den künftigen Standard für Link State Bridging braucht. Wenn man ihn (so er sich tatsächlich etabliert) einsetzt, läuft man möglicherweise Gefahr, auf eine selten genutzte Technik zu setzen und mit den ganzen Fehlern und Geburtswehen der Technik ziemlich einsam da zu stehen.

Mehr Intelligenz in die LAN-Komponenten bringen auch Mechanismen, welche für Netzmanagement und Netzanalyse genutzt werden. Da es sich bei den LAN-Switches um Komponenten handelt, die an den zentralen Schaltstellen der IT-Infrastruktur platziert sind, über die der gesamte Datenverkehr geleitet werden muss, ist es naheliegend, diese Schalt-

stellen auch für Überwachungs- und Analysezwecke zu nutzen. Funktionen hierfür erstrecken sich über ein sehr breites Spektrum: von der einfachen Sammlung statistischer Lastwerte über die Erstellung komplexerer Reports mit den Anteilen von IP-Adressen, Protokollen, TCP- und UDP-Ports am Verkehr bis hin zum kompletten Mitschnitt des Datenverkehrs. Letzteres scheitert immer wieder an der steigenden Menge der mitzuschneidenden Daten. Nichtsdestotrotz kann der Funktionsumfang der LAN-Switches auch mit Analysefunktionen aufgebohrt werden, wie in der Abbildung 3 angedeutet.

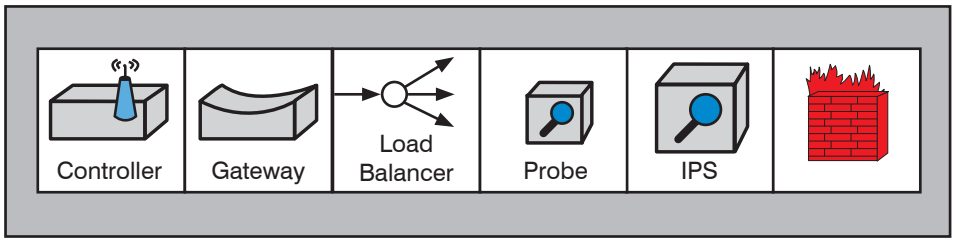


Abbildung 3: Beispiele für Switchmodule mit Zusatzfunktionen

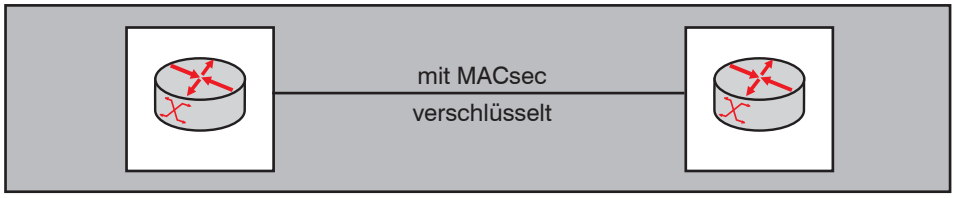


Abbildung 4: Verschlüsselung auf der Ebene der Schicht 2

Ähnlich verhält es sich mit der Wahrnehmung von Funktionen, die mit der klassischen Rolle von Layer-2- und Layer-3-Switches wenig zu tun haben, aber von einigen Herstellern auf der Basis der Switches angeboten werden. Beispiele sind Firewalls und Load Balancer als Module von Switches. Die Meinungen darüber gehen auseinander. Einige Netzbetreiber bevorzugen die Minimierung der Anzahl der zu betreibenden Geräte und konzentrieren viele Funktionen auf die Switches, während andere nicht zuletzt wegen der organisatorischen Arbeitsteilung im Unternehmen die Funktion LAN Switching nicht mit Firewalling oder Load Balancing vermischen wollen.

Weniger auf zentralen Switches und mehr am Rande des Netzes werden häufig Instanzen wie VPN Gateways oder WAN Optimiser platziert. Auch diese können als Module in Netzkomponenten (zumindest in Routern) oder aber als eigenständige Geräte zum Einsatz kommen. Zusammen mit WAN Optimising werden sogar weitergehende Funktionen wie Print Service, DHCP Service, Windows Domain Controller etc. angeboten, damit in einer Außenstelle möglichst viele Funktionen auf dasselbe Gerät konzentriert werden können. Ein Vorteil wäre die Reduzierung der Zahl der Service-Partner, mit denen Verträge für die Wartung von Geräten in Außenstellen abgeschlossen werden müssen.

Seit 2006 ist der IEEE Standard for Local and Metropolitan Area Networks Media Access Control (MAC) Security (kurz: MACsec) in Kraft. Gemäß diesem Standard kann auf der Ebene der Schicht 2 (MAC) sowohl eine Authentisierung als auch eine Verschlüsselung von Frames implementiert werden, wie aus der Abbildung 4 hervorgeht. Unterstützen die Netzkomponenten MACsec, lässt sich der Datenverkehr verschlüsseln. Ein solcher Ansatz wäre zumindest für solche Fälle attraktiv, in denen Netzverbindungen über nicht physikalisch geschützte Trassen realisiert werden. Der Abhörung der Leitung wird ein Riegel vorgeschoben. Allerdings bleiben mit MACsec andere Risiken der Kompromittierung der Daten, denn ein Angreifer kann weiterhin über die Endgeräte und Netzkomponenten auf unverschlüsselte Daten zugreifen. Es fragt sich also, wie wertvoll und sinnfällig MACsec als eine der zahlreichen neuen Funktionen von Netzkomponenten ist.

Vor dem Hintergrund der oben genannten Vielzahl der Zusatzfunktionen von Netzkomponenten, welche diese über ihre Standardrolle als Layer-2- und Layer-3-Switches hinauswachsen und zu intelligenteren Instanzen in der IT-Infrastruktur werden lassen, werden Kriterien benötigt, die einer Entscheidung für oder wider die Nutzung solcher weitergehenden Funktionen der Netzkomponenten zugrunde gelegt werden sollten.

Aus der Sicht des Autors besteht eines der wichtigsten Kriterien zur Bewertung einer Zusatzfunktion darin, dass diese Funktion die Standardisierung der Konfiguration des Netzes nicht konterkariert. Das Netz sollte möglichst einheitlich konfiguriert sein. Auch wenn die Verwendung derselben Konfiguration überall nicht möglich ist, ist an dem Ziel festzuhalten, die Vielfalt der Konfiguration zu minimieren. Der Betreiber sollte möglichst aus dem Gedächtnis die Standardkonfiguration erkennen können. Nur so wird sichergestellt, dass im Fehlerfall erstens Konfigurationsfehler schnell erkannt werden, zweitens ein „Schlechtfall“ einer möglichst großen Zahl von vergleichbaren „Gutfällen“ gegenübergestellt werden kann und drittens die Wiederherstellung einer Konfiguration innerhalb kürzester Zeit möglich ist. Außerdem trägt eine standardisierte Konfiguration erheblich zum einen zur Fehlervermeidung und zum anderen zur Minimierung des Aufwands für Installationen, Änderungen, Umzügen und Erweiterungen des Netzes bei.

Wenn also zum Beispiel die Implementierung von Network Access Control darin besteht, an allen Ports dieselben Einstellungen vorzunehmen, wäre dies tolerierbar, vorausgesetzt, diese Einstellungen verursachen keine Probleme. Fast jede der aufgeführten Zusatzfunktionen der Switches kann auf eine standardisierte Art genutzt werden oder aber zu einer solchen unübersichtlichen Konstellation führen, dass davon dringend abzuraten wäre. Ein weiteres wichtiges Kriterium ist die Vermeidung der Abhängigkeit von einem Hersteller. Hersteller können über Nacht vom Markt verschwinden oder in eine solche Schieflage geraten, die einen guten Service für ihre Kunden ernsthaft gefährdet. Der Wechsel des LAN-Herstellers sollte daher jederzeit möglich sein. Natürlich sind die Produkte der verschiedenen Hersteller nicht gleich zu bewerten. Jeder Herstellerwechsel ist auch mit Nachteilen bezüglich des Verlusts von Funktionen, der Umgewöhnung an die Bedienung neuer Produkte, des Aufwands für die Umstellung etc. verbunden. Aber diese Schwierigkeiten sollten nicht so groß sein, dass sie einen Wechsel unmöglich machen. Kein LAN-Betreiber darf sich auf Gedeih und Verderb von Alleinstellungsmerkmalen des Herstellers der Switches abhängig machen. Wenn die Nutzung der Zusatzfunktionen der Switches bedeutet, dass ein Wechsel unmöglich oder signifikant erschwert wird, ist die Nutzung der Zusatzfunktionen zu überdenken. Diese können aber genutzt werden, wenn sie zwar Vorteile im laufenden Betrieb bieten, in ihrer Gesamtheit jedoch zur Not auch verzichtbar sind.

Drittens darf man sich mit der Zusammensetzung der genutzten Zusatzfunktionen

nicht in eine Ecke hineinmanövrieren, in der man mit der eigenen LAN-Konstellation ziemlich allein da steht. Es muss immer eine Viel- oder zumindest Mehrzahl von anderen LAN-Betreibern geben, bei denen die Konstellation weitgehend gleich ist. Der Hersteller darf bei Problemen niemals behaupten können, die mit Problemen verbundene Kombination von Funktionen sei einmalig. Im Interesse einer schnellen Fehlerbehebung muss es möglich sein, zum Beispiel durch einen Software Update die weitestgehende Vergleichbarkeit von „Gutfällen" herstellen zu können. Außerdem stellt die Vergleichbarkeit einer Konstellation mit anderen sicher, dass Fehler und Probleme mit einer größeren Wahrscheinlichkeit anderswo entdeckt werden, bevor man die Konstellation bei sich umgesetzt hat.

Bei modularen Geräten kann durch die Nutzung von Zusatzmodulen für Firewalling, Analyse, WAN-Optimierung, Load Balancing etc. eine unerwünschte gegenseitige Abhängigkeit der verschiedenen involvierten Software-Komponenten entstehen. So ist es mehrfach dazu gekommen, dass eine längst fällige und funktional dringend benötigte Software-Aktualisierung auf einem Switch an der fehlenden Unterstützung der neuen Software-Version für Zusatzmodule wie Firewalls oder Load Balancer gescheitert ist. Diese unerwünschten Abhängigkeiten werden vor der Inbetriebnahme möglicherweise unterbewertet, wiegen aber häufig die Vorteile der Konzentration diverser Funktionen auf dieselben Geräte auf.

Der Autor kann die Erfahrungen mit verschiedenen LAN-Umgebungen bezüglich der Nutzung von Zusatzfunktionen in Switches so zusammenfassen: Je größer ein Netz, desto schwerer wiegen die Argumente für ein möglichst einfaches Design unter Verzicht auf Zusatzfunktionen, deren Auswirkungen auf die Komplexität eines Netzes negativer sein können als in einem kleineren Netz. Was die Betreiber kleinerer Netze an Zusatzfunktionen noch tolerieren können, kann für ein großes Netz schon zu komplex sein.

Kongress

ComConsult Netzwerk-Redesign Forum 2012
23.04. - 26.04.12 in Bad Neuenahr

Die explosionsartige Zunahme mobiler Endgeräte und Web-basierter Applikationen verändern unsere IT. Neue Architekturen für den Zugang und den Betrieb der Dienste müssen umgesetzt werden und erfordern weitreichende Änderungen in den Netzwerk-Infrastrukturen. Ohne geeignete Sicherheits-Konzepte auf Netzwerk-Ebene wird das Ganze nicht funktionieren.

Heiß diskutierte Fragen sind dabei:
- Welche Auswirkungen hat die starke Zunahme mobiler Endgeräte?
- Wie stark lassen wir Virtualisierung das Design unserer Netze bestimmen?
- Wie sehen zukünftige Zugangs-Architekturen aus?
- Was muss LAN-Technik machen, um die Voraussetzungen zu erfüllen?
- Was muss sich im WAN ändern? Brauchen wir technisch ein neues Routing-Zugangsverfahren?

Das ComConsult Netzwerk-Redesign Forum unterteilt sich in folgende Themenbereiche:
1. Analyse wesentlicher IT-Trends und Auswirkungen auf Infrastrukturen
2. Mobile Endgeräte und ihre sichere und performante Integration
3. LAN-Technologie und neue Architekturen: wie umfangreich sind die Änderungen?
4. WAN-Zugang zu und zwischen Infrastrukturen: Wie kritisch wird das Thema?
5. Basis-Infrastrukturen und ihr Betrieb
6. Optional buchbarer Vertiefungstag: VLAN-Strukturen: wo ist das Optimum

Dabei gehen wir auf eine Reihe von Streitfragen ein, die den Markt jetzt und in den nächsten Monaten bewegen werden (beobachten Sie die Diskussion auf www.comconsult-research.de).

Beispiele dafür sind:
- Bring Your Own Device: voller Zugang zu Infrastrukturen und trotzdem sicher? Macht Bring-Your-Own-Device technisch und wirtschaftlich Sinn?
- WLAN-Zukunft: 802.11n reicht für die mobile Zukunft nicht aus, aber wo liegt die Zukunft? IEEE 802.11ac kontra IEEE 802.11ad
- Verteilte und virtualisierte Strukturen: welche Konsequenzen hat das für LAN und WAN?
- Was müssen Provider in Zukunft leisten?
- LAN-Architekturen im Streit: brauchen wir die neuen Standards überhaupt, und welche Relevanz haben sie im Campus?
- VLANs zwischen Alptraum und Notwendigkeit: wie viel ist gut, ab wenn beginnt das Chaos?

Moderation: Dipl.-Inform. Petra Borowka-Gatzweiler, Dr.-Ing. Behrooz Moayeri
Kongress:: € 2.090,-- netto
Intensiv-Tag am 26.04.12: 990,-- netto
Veranstaltung mit Intensiv-Tag 23.04. - 26.04.12: € 2.490,-- netto

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

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Netzzugangskontrolle: Technik, Planung und Betrieb, 27.02. - 29.02.12 in Berlin

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

Preis: € 1.890,-- netto

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen, 27.02. - 29.02.12 in Berlin

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

Preis: € 1.890,-- netto

Datenschutz- und steuerrechtliche Aspekte von Cloud Computing, 12.03. - 13.03.12 in Bonn

Jederzeitige Verfügbarkeit der Daten und Kosteneinsparungen lassen Cloud Computing verlockend erscheinen. Wer jedoch Daten in fremde Hände geben will, muss sich über Datenschutz und Datensicherheit erhebliche Gedanken machen, da in Deutschland der Auftraggeber von IT-Dienstleistungen unabhängig von der vertraglichen Regelung die Haftung gegenüber Dritten in Bezug auf Datenverlust, unbefugter Nutzung oder sonstiger Datenschutzverletzungen übernehmen muss. Darüber hinaus gibt es zahlreiche Rechtsvorschriften, die die Speicherung in bestimmten Ländern oder den Datenzugriff aus diesen Ländern an bestimmte Voraussetzungen knüpfen oder sogar ganz verbieten.

Preis: € 1.590,-- netto

Umfassende Absicherung von Voice over IP und Unified Communications, 12.03. - 13.03.12 in Bonn

Dieses Seminar zeigt Wege auf, wie die Vorteile von Unified Communications für das Unternehmen nutzbar gemacht werden können ohne gleichzeitig die Sicherheit geschäftsentscheidender Kommunikation aufs Spiel zu setzen.

Preis: € 1.590,-- netto

WAN: Aktuelle Technologie und Erfahrungen aus Ausschreibungen, 12.03. - 13.03.12 in Bonn

Das Programm des Seminars „WAN: Neue Verfahren und Erfahrungen aus Ausschreibungen“ bietet wertvolle Tipps und Empfehlungen sowohl zu technischen als auch zu organisatorischen Aspekten der Konzeption, der Planung, der Ausschreibung und des Betriebs von Wide Area Networks. Die Referenten des Seminars blicken auf langjährige Erfahrungen im WAN-Bereich zurück und vermitteln im Seminar Erkenntnisse aus Dutzenden von Projekten, in denen Wide Area Networks entworfen, ausgeschrieben und optimiert wurden.

Preis: € 1.590,-- netto

Datenschutz- und steuerrechtliche Aspekte von Cloud Computing, 12.03. - 13.03.12 in Bonn

Jederzeitige Verfügbarkeit der Daten und Kosteneinsparungen lassen Cloud Computing verlockend erscheinen. Wer jedoch Daten in fremde Hände geben will, muss sich über Datenschutz und Datensicherheit erhebliche Gedanken machen, da in Deutschland der Auftraggeber von IT-Dienstleistungen unabhängig von der vertraglichen Regelung die Haftung gegenüber Dritten in Bezug auf Datenverlust, unbefugter Nutzung oder sonstiger Datenschutzverletzungen übernehmen muss. Darüber hinaus gibt es zahlreiche Rechtsvorschriften, die die Speicherung in bestimmten Ländern oder den Datenzugriff aus diesen Ländern an bestimmte Voraussetzungen knüpfen oder sogar ganz verbieten.

Preis: € 1.590,-- netto

Service-Spezifizierung - Grundlegende Methode für verlässliche, rationelle und rentable Service-Erbringung, 14.03. - 16.03.12 in Köln

In diesem Seminar erlernen die TeilnehmerInnen die grundlegende Methodik der Service-Spezifizierung und die durchgängige Anwendung der Service-Spezifikation.

Preis: € 1.890,-- netto

Rechenzentrumsdesign - Technologien neuester Stand, 19.03. - 21.03.12 in Köln

Das 3-tägige Seminar „Rechenzentrumsdesign – Technologien neuester Stand“ fokussiert sich auf aktuelle Technologien und Trends im Rechenzentrumsumfeld. Sie lernen von der Verkabelung über die Stromversorgung, die Klimatisierung und den Schrankaufbau, wie ein ausfallsicheres und energieeffizientes Rechenzentrum heute strukturiert wird. An den Tagen zur aktiven Netztechnik lernen Sie, welche Mechanismen für Redundanz, Lastverteilung und Standort-übergreifende Hochverfügbarkeit in aktuellen RZ-Planungen zu berücksichtigen sind und wie diese mit dem fortwährenden Trend zur Virtualisierung zusammenspielen. Abschließend werden aktuelle Speichersysteme, deren Anbindung über die am Markt verfügbaren Übertragungsprotokolle sowie Aspekte zur Datensicherung und Disaster Recovery diskutiert.

Preis: € 1.890,-- netto

Aktuelle VPN-Technik, 19.03. - 21.03.12 in Aachen

Die Nutzung von VPN-Technik hat sich in der jüngeren Vergangenheit insbesondere im Bereich des Remote Zugriffs mobiler oder auch stationärer Anwender (Stichwort: Telearbeit) auf zentrale Ressourcen als mehr oder weniger Standard-Lösungsansatz etabliert. Aber auch zur kostenoptimierten Anbindung von (typischerweise kleineren) Remote-Standorten an Corporate WAN-Strukturen bewährt sich dieser Ansatz. Dieses Seminar vermittelt die für einen erfolgreichen VPN-Einsatz notwendigen Kenntnisse der aktuell relevanten Technologien. Alle wesentlichen Bausteine typischer Lösungen werden detailliert erklärt und anhand praktischer Projektbeispiele und Übungen wird der Weg zu einer erfolgreichen VPN-Lösung aufgezeigt.

Preis: € 1.890,-- netto

Zertifizierungen

ComConsult Certified Network Engineer

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

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

Internetworking
12.03. - 16.03.12 in Aachen
11.06. - 15.06.12 in Aachen
22.10. - 26.10.12 in Aachen

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

ComConsult Certified Trouble Shooter

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

Trouble Shooting für Netzwerk-Anwendungen
20.03. - 23.03.12 in Aachen
26.06. - 30.06.12 in Aachen
04.12. - 07.12.12 in Aachen

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

ComConsult Certified Voice Engineer

Session Initiation Protocol Basis-Technologie der IP-Telefonie
26.03. - 28.03.12 in Stuttgart
18.06. - 20.06.12 in Bonn
29.10. - 31.10.12 in Bonn

Umfassende Absicherung von Voice over IP und Unified Communications
12.03. - 13.03.12 in Bonn
11.06. - 12.06.12 in Köln
01.10. - 02.10.12 in Düsseldorf

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen
27.02. - 29.02.12 in Berlin
07.05. - 09.05.12 in Hamburg
24.09. - 26.09.12 in Bonn
26.11. - 28.11.12 in Bonn

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

Basis-Paket: Beinhaltet die drei Basis-Seminare
Grundpreis: € 4.840,-- netto statt € 5.370,-- netto
Optionales Einsteigerseminar: Aufpreis € 1.190,-- netto statt € 1.590,-- netto

Impressum

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

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

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

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