ComConsult Research

# Der Netzwerk Insider

Mai 2009

Systematische Weiterbildung für Netzwerk- und IT-Professionals

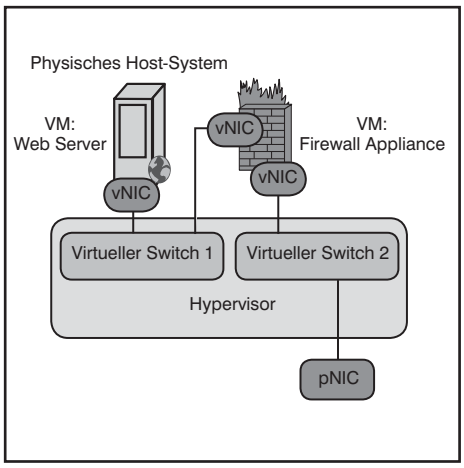
Schwerpunktthema

# Virtualisierung:

## Mehr Sicherheit durch virtuelle Firewalls?

**von Dipl.-Inform. Matthias Egerland, Dipl.-Ing. Björn Korall, Dipl.-Inform. Daniel Meinhold**

**Nachdem die Server-Virtualisierung in die meisten Rechenzentren Einzug gehalten hat, ist nun die Virtualisierung weiterer Infrastruktur-Komponenten die logische Konsequenz. Wird dieser Ansatz zielgerichtet zu Ende gedacht, gipfelt er in Konzepten wie „Office-in-a-Box“ bzw. „Datacenter-in-a-Box“. Ein besonderes Augenmerk ist bei der Virtualisierung weiterer Rechenzentrumsbestandteile auf Sicherheitselemente zu richten, da diese naturgemäß besonderen Anforderungen hinsichtlich Funktionalität, Verfügbarkeit und Leistung unterliegen.**




Im Rahmen dieses Artikels werden die Auswirkungen von virtuellen Firewalls auf die Rechenzentrumsinfrastruktur betrachtet. Hierbei liegt der Schwerpunkt auf dem Einfluss, den Firewalls auf Aspekte des Netzdesigns und des Netzwerkmanagements haben, wenn sie in Form von virtuellen Maschinen innerhalb einer Server-Virtualisierungslösung laufen. Letztlich hängt die Sicherheit auch in einer virtualisierten Umgebung nicht allein von den Leistungsmerkmalen der Sicherheitskomponenten ab, sondern auch entscheidend von der Komplexität und der Managebarkeit des Gesamtsystems.

weiter auf Seite 19

Zweitthema

# MS Office Communications Server:

## Total Cost of Ownership im Vergleich zu klassischen Unified-Communications-Lösungen - Teil 2

**von Dr. Michael Wallbaum und Dr. Frank Imhoff**

**Um die Gesamtkosten einer modernen Unified-Communications-Lösung gegenüberzustellen, müssen zahlreiche Faktoren einkalkuliert werden. Dazu gehören Wartungs- und Servicekosten ebenso wie Strom, Kühlung, Netzwerk-Anbindungen, Redundanz-Maßnahmen u.v.a.m. Gleichzeitig sind zwar deutliche Einspareffekte mithilfe von Unified Communications (UC) zu erzielen, jedoch sind diese Effekte schwer zu generalisieren und im Vorhinein kaum bezifferbar. Das liegt vor allem an fehlenden Erfahrungswerten, aber auch an der Tatsache, dass die Einführung von UC individuell auf jedes Unternehmen abgestimmt werden muss.**

Zunächst bleibt also nur, die reinen Kosten im Sinne der Total Cost of Ownership (TCO) verschiedener UC-Lösungen zu betrachten. Im ersten Teil dieses Artikels haben wir bereits Lösungsansätze der Hersteller Cisco, Siemens Enterprise Networks (SEN) und Microsoft für drei verschiedene Nutzer-Szenarien gegenübergestellt.

weiter auf Seite 8

Sommer-Highlights

## IT-Sicherheits-Forum 2009

## Netzwerk-Design-Wettbewerb 2009

ab Seite 4

Geleit

## Brauchen wir überhaupt Sicherheits-Lösungen?

ab Seite 2

Aktuelle Reports

## Wide Area Networks:

**Technik und Funktionsweise**

**+**

**Leitfaden für Design, Ausschreibung und Betrieb**

ab Seite 17

Zum Geleit

# Brauchen wir überhaupt Sicherheits-Lösungen?

Die Argumentation der Verkäufer von Sicherheits-Lösungen hat etwas Ermüdendes. Danach sind wir umzingelt von Bedrohungen und können uns glücklich schätzen, wenn wir überhaupt noch im Besitz einer lauffähigen IT-Lösung mit privaten Daten sind. Tatsächlich leidet die gesamte Branche unter dem Problem, dass immer wieder in der Vergangenheit Bedrohungs-Szenarien konstruiert worden sind, die in der Praxis bedeutungslos waren. Dies führt über die Zeit zwangsläufig zu einer Abstumpfung auf der Kundenseite. Kernproblem bleibt die Frage der Motivation eines Angreifers und warum er gerade dieses Unternehmen überhaupt angreifen sollte.

Tatsächlich muss unterschieden werden zwischen einem bewussten Angriff auf ein Unternehmen und einem unbewussten zum Beispiel durch ein Robot- /Virenverteilsystem. Die Bedrohung durch Robot- und Virenverteilsysteme muss ohne Frage als gegeben angesehen werden (u.a. als Teil der Technik von SPAM und DoS-Betreibern). Die meisten Unternehmen werden dabei gegen die gängigen Ausprägungen dieser Angriffe gewappnet sein. Bei dem bewussten Abgriff gibt es ganz unterschiedliche Formen des Angriffs, als Beispiele sind zu nennen:

- die gezielte Sabotage (zum Beispiel von Webservern)
- Spieltrieb innerhalb der Hacker-Community
- der gezielte Versuch des Datendiebstahls oder der Datenmanipulation

Die Dimension des Diebstahls vertraulicher Informationen muss in jedem Fall separat betrachtet werden, da die Absicherung dieses Bereichs ein weiter gefasstes Konzept erfordert und auch eine Menge nicht technischer Elemente beinhaltet. Tatsächlich wird es für einen Angreifer in diesem Bereich in der Regel eine Option sein, die traditionellen Angriffsformen zu benutzen (Einschleusung bzw. Nutzung eines Mitarbeiters durch Bestechung, Bedrohung...).

Wie real ist nun das Risiko, in dem sich ein Unternehmen befindet, wirklich? Ein wesentlicher Punkt in der Risikobewertung ist die Einfachheit des Angriffs. Wie hoch sind die technischen Hürden, die der Angreifer tatsächlich zu nehmen hat? Für sehr professionelle Angreifer wird die Frage gar nicht so entscheidend sein (diese werden im Zweifelsfall sowieso mit einem anderen Portfolio von Angriffsinstrumenten arbeiten), aber für die Frage, wie viele weniger professionelle Angreifer Zugang zum Unternehmen erhalten, ist dies der zentrale Knackpunkt.

Und auch ohne in das permanente Predigen von Bedrohungen mit einfallen zu wollen, ist gerade in diesem Bereich zur Zeit eine messbare und deutliche Veränderung zu beobachten. Tatsächlich sind wir in Mitten einer Technologie-Veränderung, die die Hürden für einen Angreifer senkt oder die Menge seiner Möglichkeiten erhöht. Betroffen davon sind u.a. die zentralen Infrastrukturen der Unternehmen und nicht nur die Endgeräte.

Wesentliche Bereiche, in denen wir diese Veränderungen beobachten können, sind:

- die Rechenzentren im Übergang zu Virtualisierung
- mobile Mitarbeiter und deren technische Einbindung in das Unternehmen
- der langsame, aber stetige Ausbau von Unified Communications
- die zunehmende Integration von Produktionsanlage in offene Netzwerk-Infrastrukturen

## Brauchen wir überhaupt Sicherheits-Lösungen?

- die lawinenartige Ausbreitung von Webanwendungen, dabei speziell die schnelle Etablierung von AJAX

- die Wandlung der Bedeutung von Browsern hin zu Laufzeitumgebungen für Anwendungen

Diese Entwicklungen sind alle für Unternehmen wichtig und zu begrüßen. Sie erhöhen Effizienz und senken Kosten, sie verbessern die Schnittstelle zum Kunden. Aber: alle diese Entwicklungen gehen einher mit einer deutlichen Vereinfachung der Umsetzung eines Angriffs. Einige Beispiele, die sicher nicht vollständig sind, sollen das unterstreichen:

- Virtualisierung hebt die bisherigen Grenzen zwischen Servern auf. Gleichzeitig wird die bisherige Statik der Server-Architektur durch ein dynamisches System wandernder Prozesse und Server abgelöst. Es entstehen neue Zugangs-Möglichkeiten und gleichzeitig wird die Absicherung schwerer. Tatsächlich fehlen allen bestehenden Virtualisierungs-Plattformen geeignete Hilfsmittel schon auf Netzwerk-Ebene

- Mobile Mitarbeiter sollen an jedem Ort in alle Unternehmens-Prozesse einbindbar sein, dies erfordert, dort auch entsprechende Daten und Applikationen verfügbar zu machen

- Ein Kernmerkmal von Unified Communications ist der dynamische Wechsel zwischen Medien, der Übergang von IM zu Sprache und Video, die Einbindung von Präsentationen, White-Boards, Desktop-Sharing und vielen anderen Elementen. Dies geht einher mit dem durchaus wichtigen Ziel, externe Kommunikationspartner in dieses System einzubinden. Anders formuliert: nie war es einfacher, umfassende Information nach außen zu bringen

- Produktionsanlagen sind der am weitesten ungeschützte Teil unserer Infrastrukturen. Sie sind es, weil es nie einen IT-technischen Bedarf des Schutzes in der Vergangenheit gab. Die technischen Systeme waren Hersteller-spezifisch und sowieso nach außen geschlossen. Mit dem Siegeszug von Ethernet und auch der Einbindung von UC in diese Umgebungen öffnen wir eine Welt, die darauf nicht vorbereitet ist.

- Der in jedem Fall leicht verständliche Bedarf, Webanwendungen in die gleiche Qualität der Bedienung wie Desktop-Anwendungen zu führen, hat zur extrem schnellen Entwicklung neuer Technologien geführt. Ein wesentliches Beispiel ist AJAX. Es liegt in der Natur von AJAX, mit anderen Systemen und Plattformen zu kommunizieren. Es liegt in der Natur von Webanwendungen allgemein, dass ihr Programmiercode in weiten Bereichen offen liegt. Daraus resultieren eine ganze Reihe von Angriffsmöglichkeiten

- Die Veränderung der Browser-Technologie erfolgt für viele Anwender unbemerkt. Google hat mit Gnome die Basis für eine Laufzeitumgebung für hochperformante Webanwendungen gelegt. Apple ist mit Safari 4 gefolgt (zur Zeit noch Beta). Microsoft hat mit dem Übergang von Internet Explorer 7 zur Version 8 nachgezogen, auch wenn der Internet Explorer immer noch deutlich langsamer ist als andere Browser. Aber eines wird in dieser Entwicklung klar: hier kommt eine Lawine neuer Anwendungen auf uns zu. Anwendungen, die in der Vergangenheit gar nicht umsetzbar waren, weil die technische Basis fehlte. Anwendungen der Zukunft sind eine Mischung aus Browser-Plugins, Java-Code auf Servern und AJAX. Unser gesamtes Sicherheits-Verständnis ist darauf nicht vorbereitet. Ebenso sind diese neuen Technologien nicht sensitiv gegenüber Sicherheit, häufig wird das Thema einfach ignoriert (siehe auch entsprechende Diskussionen in den AJAX-Communities)

Alle diese – bei Weitem nicht vollständigen – Beispiele zeigen, dass die technische Hürde für Angreifer sinkt. Damit kommen wir zurück zur Ausgangsfrage: brauchen wir überhaupt Sicherheits-Lösungen? Die Antwort ist entsprechend der zuvor genannten Beispiele: mehr denn je. Aber wir müssen weg von diesem unspezifischen Bedrohungs-Geschwätz der Vertreiber einzelner Produkte. Wir müssen hin zu einer Praxis-relevanten Einschätzung der Bedrohungs-Situation und zur Entwicklung vom Gesamt-Konzepten, die dieser Einschätzung gegenüber angemessen und wirtschaftlich sind.

Unser Beitrag als ComConsult Research zu diesem Thema ist das ComConsult IT-Sicherheits-Forum 2009. Hier diskutierten wir die Veränderungen der genannten Technologien und deren Relevanz für die Bedrohungs-Situation. Hier diskutieren wir auch die zentrale Frage, wie man zu einem Praxis-relevanten und angemessenen Gesamtkonzept kommt.

Ihr
Dr. Jürgen Suppan

**Bemerkung zum Artikel „IT-Verkabelung im Rechenzentrum: Beginn einer neuen Epoche?“ aus dem Netzwerk Insider Ausgabe März 2009**

In der März Ausgabe des Netzwerk Insiders im Artikel „IT-Verkabelung im Rechenzentrum: Beginn einer neuen Epoche?“ von Herrn Kell wurde auf die hohen Kosten des GG45, einer genormte Kategorie-$7_A$ Buchse, eingegangen. So war dort der Satz zu lesen, „dass der Einsatz des GG45 zu einem ca. 3-fach höheren Preis der gesamten Anschlusstechnik führt“. Da dies zu einer missverständlichen, vom Autor nicht beabsichtigten Interpretation führen kann, erfolgt nachstehend eine genauere Kostenbetrachtung:

Zur gesamten Verkabelung gehören, neben der modularen Anschlussbuchse (RJ45, GG45...) die Komponenten Horizontalkabel, Leerpanel zur Aufnahme der Buchsen, leere Wanddosen und Patchkabel. Diese bilden, zusammen mit den Aufwendungen für die Installation, die Gesamtkosten der passiven Verkabelung.

Wenn man die Kosten einer Kat.$6_A$ Verkabelung mit denen einer durchgängigen Kat.$7_A$ vergleicht, so ist es notwendig, alle Komponenten der gesamten Verkabelung dem Vergleich zu unterziehen und zum Ende die Gesamtkosten der Verkabelung zu bewerten. Gemäß aktueller BSRIA Studie (April, 2009), werden in Deutschland zu 83% Kat.7/-$7_A$ Kabel installiert, zumeist jedoch mit RJ45 Buchsen. Daraus folgt, dass der größte Kostenblock – das Horizontalkabel – in beiden Fällen identisch ist. Auch die Leerpanel und Wanddosen sind im Vergleich kostenneutral. Richtig ist jedoch, dass eine GG45 Buchse als Einzelkomponente ca. Faktor 3 teurer ist. Außerdem ist die Montage aufwändiger, was natürlich ebenfalls zu höheren Kosten im Vergleich führt. Nach langjährigen Projekterfahrungen von Nexans liegen die Mehrkosten der gesamten Verkabelung unter Einsatz von GG45 bei ca. 30% - 40%. Diese Mehrkosten können seitens des Autors auf Basis vergleichender Ausschreibungen bestätigt werden. Selbstverständlich bietet eine Kategorie-$7_A$-Verkabelung bedingt durch den größeren bereitgestellten Frequenzbereich einen technischen Mehrwert und darf deshalb nicht ausschließlich über den Mehrpreis bewertet werden.

Sonderveranstaltung

# Netzwerk-Design-Wettbewerb 2009

## Alcatel-Lucent, Brocade/Foundry, Cisco, Enterasys, Extreme, H3C/3com, HP, Juniper und Nortel stellen sich dem Vergleich

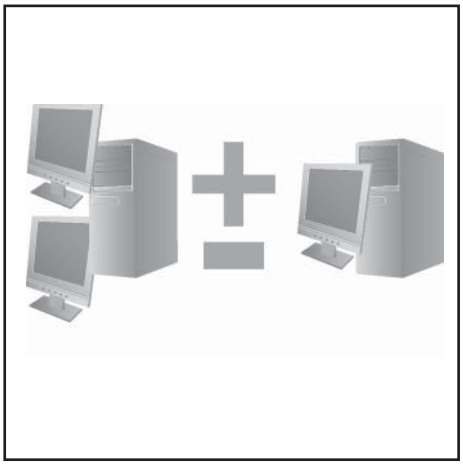
**Die ComConsult Akademie veranstaltet vom 25. - 26.05.09 ihre Sonderveranstaltung „Netzwerk-Design-Wettbewerb 2009“ in Köln.**

Netzwerk-Standards legen Verfahren fest, die eine offene Kommunikation zwischen Geräten verschiedener Hersteller garantieren. Aber Standards legen nicht fest:

- Geräte-Ausstattungen
- Geräte-Qualitäten
- Portdichten
- Verfügbarkeit von speziellen Geräte-Typen
- Design-Grundsätze
- Eingesetzte Bandbreiten
- Genutzte und bevorzugte Redundanz-Verfahren
- Einbindung in Konfigurations- und Management-Lösungen
- Einbindung in Sicherheits-Lösungen

So ist es nicht überraschend, dass es nach wie vor erhebliche Unterschiede bei den Gesamt-Portfolios und Einzelprodukten verschiedener Hersteller gibt.

Der ComConsult Research Netzwerk-Design-Wettbewerb 2009, der von UBN durchgeführt wurde, deckt diese Unterschiede auf. Er zeigt für die 9 Hersteller, die sich am Wettbewerb beteiligt haben:



- welche Schwerpunkte im Design und in der Auslegung existieren
- wo ein Optimum aus Preis/Leistung zu erwarten ist
- wo Schwachstellen in den Produktfamilien liegen

Im Ergebnis ist dieser Design-Wettbewerb ein wichtiger Beitrag zur Absicherung Ihrer bestehenden und zukünftigen Investitionen.

Basierend auf einem realisitischen Projekt-Szenario in Form eines RFI (Request for Information in der Anlage) haben die Hersteller detaillierte Planungen für das Szenario entworfen und umfangreiche Funktionslisten für alle angebotenen Produkte bearbeitet. Die Ergebnisse zeigen deutliche Unterschiede zwischen den Herstellern.

Dabei geht der Wettbewerb auch unabhängig von konkreten Produkten auf die Fragen ein:

- wie sieht ein aktuelles Design aus?
- welche sinnvollen Design-Varianten bestehen?
- wo gibt es Meinungsverschiedenheiten zwischen Planern und Herstellern?
- welche Mängel müssen im Design berücksichtigt werden?
- in welche Richtung gehen die zukünftigen Trends?

Sie erhalten eine absolut neutrale und einmalige Chance, den Status Ihres bestehenden Netzwerk-Designs zu prüfen, Fragen direkt an die Hersteller zu richten und die neuesten Erkenntnisse zum Thema Planung und Design in zukünftige Investitionen einfließen zu lassen.

Durch diese Sonderveranstaltung führt Sie Frau Dipl.-Inform. Petra Borowka.

Sichern Sie sich rechtzeitig einen Platz!

Fax-Antwort an ComConsult 02408/955-399

# Anmeldung

## Netzwerk-Design-Wettbewerb 2009

Ich buche das Seminar
**Netzwerk-Design-Wettbewerb 2009**
☐ 25.05. - 26.05.09 in Köln
zum Preis von 1.690,- € zzgl. MwSt.

☐ Bitte reservieren Sie für mich ein Hotelzimmer im NH Köln-City

vom_____ bis_____09

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

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

ComConsult IT-Sicherheits-Forum 2009

# ComConsult IT-Sicherheits-Forum 2009

**Die ComConsult Akademie veranstaltet vom 22.06. - 25.06.09 ihren Kongress „IT-Sicherheits-Forum 2009“ in Königswinter.**

Das ComConsult Sicherheitsforum 2009 gibt einen umfassenden Überblick über den Stand moderner und erprobter Sicherheitstechnologien. Basierend auf den ermittelten Kernbereichen führen Top-Experten der Sicherheitstechnik von der Bedrohungslage zur praxiserprobten Umsetzung geeigneter Sicherheitslösungen.

Die Umsetzung von Sicherheits-Lösungen steht immer wieder und immer mehr vor folgenden Herausforderungen:

- Zunahme der Zentralisierung und Integration von Technologien
- Immer mehr verschiedene Technologien als Nutzer einer gemeinsamen Infrastruktur
- Zunahme der Abhängigkeiten und Wechselwirkungen zwischen Technologien

ComConsult Research hat deshalb exklusiv zum ComConsult Sicherheitsforum 2009 aktuelle Sicherheitsprojekte analysiert und die Schlüsseltechnologien herausgearbeitet, die angepackt werden müssen, um Sicherheit auch Technologieübergreifend realisieren zu können.

Dabei hat ComConsult Research die folgenden Bereiche als aktuell prägend für die erfolgreiche Umsetzung von Sicherheitsprojekten identifiziert:

- Virtualisierung und RZ-Redesign
- Netzwerk-Technologien
- Integration mobiler Geräte
- Voice und Unified Communications
- Webanwendungen
- Email
- Netzintegrierte Produktionsanlagen

Das ComConsult Sicherheitsforum 2009 geht intensiv auf diese Bereiche und deren zukünftige Entwicklung ein, analysiert die technischen Probleme und vergleicht die bestehenden Lösungsmöglichkeiten. Das Ganze wird in den Rahmen einer umfassenden Gesamtkonzeption gestellt, wobei auch die Frage der Prüffähigkeit der Lösung nach IT-Grundschutzhandbuch und ISO 27001 diskutiert wird.

Durch dieses Forum führt Sie Dr. Simon Hoff. Er 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.

Fax-Antwort an ComConsult 02408/955-399

# Anmeldung
# IT-Sicherheits-Forum 2009

Ich buche den Kongress
**ComConsult IT-Sicherheits-Forum 2009**

☐ **ohne Workshop**
22.06. - 24.06.09 in Königswinter
zum Preis von € 1.890,- zzgl. MwSt.

☐ **mit Workshop (bitte auswählen)**
22.06. - 25.06.09 in Königswinter
zum Preis von € 2.290,- zzgl. MwSt.

**Workshopauswahl**

| **vormittag** | **nachmittag** |
|---|---|
| ☐ 1 | ☐ 1a |
| ☐ 2 | ☐ 2a |
| ☐ 3 | ☐ 3a |

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

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

# Programmübersicht ComConsult IT-Sicherheits-Forum 2009

## Montag, 22.06.09

**9:30 Uhr - 10:30 Uhr**
**Keynote: IT-Sicherheitsarchitektur unter Berücksichtigung aktueller Trends**
- Aktuelle IT Trends und ihre Auswirkung auf die Informationssicherheit
  - Virtualisierung, Voice over IP und Unified Communications, Mobilität
- Bedrohungslage 2009: Unsichere Browser, unerwünschte Kommunikation, schadensstiftende Software
- Sichere Netze als Megatrend der nächsten Jahre: Authentisierung, Integrität und Verschlüsselung als Service im Netz

*Dr. Simon Hoff, ComConsult Beratung und Planung GmbH*

**11:00 Uhr - 11:45 Uhr**
**Erfahrungen bei der Anwendung von IT-Grundschutz und ISO 27001**
- Projektbeispiele zu folgenden Punkten: BSI-Grundschutz-Zertifizierung, BS27001-Zertifizierung, Sicherheitsanalysen und Konzepterarbeitungen auf Basis BSI-Standards 100-1 bis 100-3
- Wie eine Zertifizierung effizient vorzubereiten ist
- Was die Haupt-Knackpunkte sind
- Worauf Prüfer besonderen Wert legen
- Nicht nur saure Pflicht: die Vorbereitung hilft, sich gezielt zu verbessern
- Das Rad mehrfach erfinden oder Synergieeffekte - Sicherheitsaudits, Revision, branchenspezifische Auflagen, S-OX u.ä.
- Auch ohne Zertifizierung: die Grundschutz-Systematik als nützliches Hilfsmittel

*Oliver Flüs, ComConsult Beratung und Planung GmbH*

**11:45 Uhr - 12:45 Uhr**
**Sicherheit in virtualisierten Umgebungen**
- Herausforderung Virtualisierung: Betriebssystemsicherheit, Datenintegrität und Vertraulichkeit in virtualisierten Umgebungen
- Sicherheitskonzepte von Virtualisierungslösungen: die führenden Anbieter zur Servervirtualisierung im Vergleich
- „Virtuelle Sicherheit"? Was leisten Schnittstellen zum Virenschutz als Teil des Hypervisors?
- Vom einfachen Paketfilter bis zum Unified Threat Management: virtuelle Sicherheits-komponenten als virtuelle Maschine auf dem Host-System
- Virtuelle Sicherheitskomponenten: Integration in virtualisierte Umgebungen, Chancen und Risiken dieses Architekturwandels

*Matthias Egerland, Comconsult Beratung und Planung GmbH*

**14:15 Uhr - 16:15 Uhr**
**Sicherheit der Virtualisierungslösungen im Vergleich**
Referenten von den Herstellern von Virtualisierungslösungen mit anschließender Podiumsdiskussion

**16:45 Uhr - 17:30 Uhr**
**Windows 7: Sicherheitsneuerungen**
- Was ändert sich mit Windows 7?
- Gemeinsamkeiten mit Vista
- Werden die Probleme von Vista tatsächlich behoben?
- Breiterer 64-bit Support – auch von Drittherstellern (z.B. biometrische Authentisierung)
- BitLocker im neuen Gewand und BitLocker „To Go" für Wechseldatenträger
- Windows denkt mit: Action Center und automatische Erinnerung zur Sicherung von EFS Zertifikaten

*Michael van Laak, Comconsult Beratung und Planung GmbH*

**10:30 - 11:00 Uhr Kaffeepause**
**12:45 - 14:15 Uhr Mittagspause**
**16:15 - 16:45 Uhr Kaffeepause**
**ab 18:00 Uhr Happy Hour**

## Dienstag, 23.06.09

**9:00 Uhr - 9:45 Uhr**
**IT-Sicherheit für netzintegrierte Produktionsanlagen**
- Gefährdungen durch die Netzintegration von Produktionsanlagen
- Einsatz von Firewalltechniken und zugehörige Netzarchitekturen
- Absicherung auf Ebene der Endgeräte und der Netzelemente
- Sonderrolle von WLAN und anderen drahtlosen Kommunikationstechniken
- Einsatz und Grenzen von Security Scannern
- Verfügbarkeit kontra Sicherheit

*Dr. Simon Hoff, ComConsult Beratung und Planung GmbH*

**9:45 Uhr - 10:30 Uhr**
**Sichere Netzarchitektur**
- Was bedeutet die Virtualisierung für die Netzarchitektur?
- Wo gehören die Sicherheitsmechanismen hin: in die Applikationen, auf die Betriebssysteme oder ins Netz?
- Virtualisierte Netzarchitektur
- Folgen der Netzkonvergenz in Rechenzentren für die IT-Sicherheit
- Netztrennung kontra Policy-based Access Control: Was ist das bessere Konzept?
- Sind die Netze sicher genug für VoIP und Unified Communications?

*Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH*

**11:00 Uhr - 12:00 Uhr**
**Von der Geräteauthentisierung bis zu sicheren Netzen**
- Tücken der dynamischen Zuordnung von Endgeräten in mandantenfähigen Netzen
- Grenzen der reinen Geräteauthentisierung
- MAC Security gemäß IEEE 802.1AE
- Ausblick auf die neue Version von IEEE 802.1X
- Pre-Standard-Lösungen und was gibt es neben Cisco TrustSec?
- Konsequenzen für den Aufbau von Sicherheitszonen

*Dr. Simon Hoff, ComConsult Beratung und Planung GmbH*

**12:00 - 12:45 Uhr**
**Sicherheit in drahtlosen Kommunikationssystemen**
- Das Ende von WPA und TKIP
- Wie man WLAN ordentlich absichert
- Bluetooth-Sicherheit
- Kompromittierung von DECT und die Konsequenzen
- Sicherheitsaspekte bei RFID und Lokalisierungssystemen
- Blick über den Tellerrand: ZigBee, NFC und Konsorten

*Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH*

**14:00 Uhr - 14:45 Uhr**
**Herausforderung Mobilität und wie ihr zu begegnen ist**
- Gefahren durch immer mehr Daten auf immer intelligenteren mobilen Geräten
- Sicherheitskonzepte im Vergleich: Blackberry, Windows Mobile, Symbian, ...
- Wie lassen sich mobile Geräte sicher managen?
- Neue Leitlinien des BSI im Mobilfunkbereich

*Dr. Frank Imhoff, ComConsult Beratung und Planung GmbH*

**14:45 Uhr - 15:30 Uhr**
**Gesetz über die Vorratsdatenspeicherung: Was müssen Unternehmen tun?**
- Voice over IP Speicherpflichten- Bestandsdaten oder Verkehrsdaten?
- Speicherpflichten bei E-Mail-Postfächern
- Speicherpflichten bei WLAN-Zugängen
- Kostentragung der Speicherung

*Ulrich Emmert, e/s/b Rechtsanwälte*

**16:00 Uhr - 17:00 Uhr**
**Sicherheit bei Voice und Unified Communications**
- Muss Voice over IP verschlüsselt werden?
- Session Border Controller: warum eine neue Klasse von Systemen erforderlich ist
- Ist SPIT eine ernste Gefahr? Schutzkonzepte dagegen
- Gefahren durch Unified Communications
- Tauglichkeit von Skype für den Unternehmenseinsatz
- Neue Leitlinien des BSI im TK-Bereich

*Dr. Michael Wallbaum, ComConsult Beratung und Planung GmbH*

**10:30 - 11:00 Uhr Kaffeepause**
**12:45 - 14:00 Uhr Mittagspause**
**15:30 - 16:00 Uhr Kaffeepause**

## Mittwoch, 24.06.09 - vormittag

**9:00 Uhr - 9:45 Uhr**
**Unified Communications: Überwinden von Grenzen**
- Firewall-Techniken und Unified Communications
- Beispiel Video-Konferenz: Lässt sich eine Kommunikation auch über Unternehmensgrenzen hinaus sicher gestalten?
- Sichere Einbindung von Heimarbeitsplätzen und externen Kommunikationspartnern

*Michael Thissen, Tandberg*

**9:45 Uhr - 10:45 Uhr**
**Sicherheit bei Kommunikations- und Kollaborationslösungen von Microsoft**
- Sicherheit beim Microsoft Office Communications Server 2007 R2
- Sicherheit beim Microsoft Office Sharepoint Server:
- Sicherheit und Zugriffsschutz bei der SharePoint Suche
- Benutzer-Berechtigungen im Portal und in Bibliotheken
- Überwachungsmöglichkeiten im SharePoint-Portal
- Sicherheit bei Microsofts Online Services

*Markus Holländer, Lars Kuhl, ComConsult Beratung und Planung GmbH*

**11:15 Uhr - 12:00 Uhr**
**Fortschrittliche SQL Injection in Webanwendungen**
- Bedrohungen durch SQL Injection
- Unterschiede Oracle & MySQL & SQLServer
- Grundlagen Oracle SQL Injection
- Neue Möglichkeiten (XML, Tabelleninhalte in Fehlermeldungen)
- Suche nach Daten (z.B. Kreditkarten) via reguläre Ausdrücke in SQL Injection
- Lesen von Dateien via SQL Injection
- Ausführen von Betriebssystemkommandos

*Alexander Kornbrust, Red-Database-Security GmbH*

**10:45 - 11:15 Uhr Kaffeepause**

Der Veranstalter behält sich Änderungen im Programm vor!

# Programmübersicht ComConsult IT-Sicherheits-Forum 2009

## Mittwoch, 24.06.09 - nachmittag

**12:00 Uhr - 12:45 Uhr**
**Sicherheitsaspekte Dienst-orientierter Architekturen**
- Von SOA über SaaS bis Cloud Computing: Konkurriende Konzepte oder Begriffsverwirrung?
- Unscheinbar und gefährlich im Hintergrund: XML, SOAP und AJAX
- Marktübersicht: Dienste im Netz
- Technische und rechtliche Grundlagen des Dienst-Outsourcings
- Sicherheit in Unternehmen zwischen Anspruch und Wirklichkeit
- Auswahlkriterien für sicheres Outsourcing

*Dr. Michael Wallbaum, ComConsult Beratung und Planung GmbH*

**14:00 Uhr - 14:45 Uhr**
**E-Mail-Sicherheit in großen heterogenen Umgebungen**
- Problematik E-Mail-Sicherheit
- Zentrale Lösung: Gateway-Verschlüsselung
- Projekterfahrungen bei der Umsetzung von Praxis-Anforderungen
- Berücksichtigung heterogener IT-Umgebungen
- Unsichere WAN-Transferstrecken
- Einbeziehung der vorhandenen Betriebs-Ressourcen
- Testszenarien und Integration in den laufenden Betrieb
- Skizzierung der Lösungen, Realisierung

*Dr. Torsten Johr, GAI NetConsult Gmb*

**14:45 Uhr - 15:30 Uhr**
**Zentralisierte E-Mail-Sicherheit durch Virtuelle Poststellen**
- Anforderungen an sichere E-Mail und Probleme clientbasierter Lösungen
- Virtuelle Poststellen: Prinzip und Eigenschaften
- Integration Virtueller Poststellen in E-Mail-Architekturen
- Wesentliche Aspekte der Migration vorhandener Lösungen

*Dipl.-Inform. Andreas Meder, ComConsult Beratung und Planung GmbH*

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

## Donnerstag, den 25.06.09 - Praxis-Workshoptag (Optional) - Bitte kreuzen bei Wunsch jeweils einen Workshop an

### vormittags 9:00 - 11:15 Uhr

**1 Workshop 1: Sichere Netze**

- Rogue device insertion, Identitätsübernahme, DHCP- und TCP-Angriffe: Welche Gefährdungen im LAN wirklich revant snd
- Unterschiede der Implementierung von IEEE 802.1X zwischen den Herstellern: Von Po-licy-based NAC bis zur simultanen Authentisierung mehrer Endgeräte an einem Port
- CDP/LLDP & Co.: ja oder nein?
- Sicherheitsmechanismen auf Ebene der Switches und Router: Dynamic ARP inspection, IP source guard, Unicast Reverse Path Forwarding und Routing Authentication
- Management-VRF: ja oder nein? Oder Outband Management?
- Mit Live-Beiträgen der Hersteller

*Dr. Simon Hoff, Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH*

**2 Workshop 2: Mehr Sicherheit durch virtuelle Firewalls?**

Nahezu alle führenden Firewall-Hersteller bieten heutzutage eine virtualisierbare bzw. eine virtuelle Sicherheitskomponente an. Dabei unterscheiden sich die technischen Realisierungsansätze genauso stark wie das etablierbare Sicherheitsniveau. Gemeinsam mit den Herstellern wird in diesem Workshop diskutiert:

- Wie unterscheiden sich die Architekturmodelle zur Virtualisierung von Sicherheitskomponenten?
- Was leistet eine virtualisierte/virtuelle Sicherheitskomponente?
- Welche Vorteile ergeben sich aus der Virtualisierung?
- An welche Grenzen stößt die virtualisierte/virtuelle Sicherheitskomponente?
- Welche organisatorischen Abläufe müssen durch die Virtualisierung neu gestaltet wer-den?

*Matthias Egerland, ComConsult Beratung und Planung GmbH*

**3 Workshop 3: Notfallmanagement im IT-Bereich**

Mit kleinen Praxis- und Diskussionsbeispielen zu Notbetriebsformen, Notfall-relevanten Dokumenten und Rückführung auf Tagesgeschäft-Erfahrung; kommender BSI-Standard 100-4

- Flexibler Notfallprozess statt statischer Szenarienbewältigung
- IT ist komplex geworden - Prioritäten setzen und Notbetriebsformen planen
- Wichtige Notfall-relevante Dokumente - was müssen sie leisten
- Das Unerwartete erwarten - und vorbereitet sein
- Im Notfall ist alles anders - das kann nicht sein: Bewährtes aus dem Tagesgeschäft nutzen
- Ausblick und Diskussion: der neue BSI-Standard 100-4

*Oliver Flüs, ComConsult Beratung und Planung GmbH*

### nachmittags 11:45 - 15:30 Uhr

**1a Workshop 1a: Wireless Security**

- WLAN-Absicherung mit IEEE 802.1X und EAP: Konfigurationsbeispiele und Traces
- Wie sicher ist WPA Personal?
- Das Ende von TKIP, wie gelingt die Migration nach AES reibungslos?
- Hotspot-Security
- WLAN Guest Access, die Hintertür ins Corporate LAN?
- Alte und neue Angriffe auf Bluetooth und wie man sich davor schützt
- Bluetooth und Windows 7: Was gibt es hier neues?

*Dr. Joachim Wetzlar, Björn Korall, ComConsult Beratung und Planung GmbH*

**2a Workshop 2a: Sichere Oracle-Architekturen und sichere Anwendungsentwicklung**

- Typische Architekturen (RAC, HA-Lösungen, Streams, Data Guard, ...) und deren Security Probleme
- Typische Anwendungsarchitektur und typische Security Probleme
- Test-, Staging und Produktionssysteme (Cloning, Verschlüsselung, ...)
- Verschlüsselung - Auf welcher Ebene soll/muss wie verschlüsselt werden (Applikation, Datenbank, Netzwerk, Betriebssystem)
- Typische Probleme bei der Software-Entwicklung mit Oracle
- Source-Code Review

*Alexander Kornbrust, Red-Database-Security GmbH*

**3a Workshop 3a: Telekommunikationsüberwachung und Datenschutz**

- Welche Mitarbeiterdaten dürfen aufgezeichnet werden?
- Wie dürfen Telekommunikations- und Mitarbeiterdaten genutzt und ausgewertet werden?
- Wie können oder müssen Handy- und Voice-over-IP-Daten aufgezeichnet und geschützt werden?
- Was ist bei Telekom und Bahn falsch gelaufen?

*Ulrich Emmert, esb Rechtsanwälte*

**11:15 - 11:45 Uhr Kaffeepause**
**12:30 - 14:00 Uhr Mittagspause**
**15:30 Uhr Ende der Veranstaltung**

Zweitthema

# MS Office Communicati-ons Server:

# Total Costs of Owner-ship im Vergleich zu klassischen Unified-Communicati-ons-Lösungen - Teil 2

Fortsetzung von Seite 1

Dr. Michael Wallbaum ist Senior Consultant der ComConsult Beratung und Planung GmbH. Er blickt auf jahrelange Projekterfahrung in Forschung, Entwicklung und Betrieb im Bereich mobiler Kommunikationssysteme, Voice-over-IP und Groupware zurück. Zu diesen Themenbereichen sind von ihm zahlreiche Veröffentlichungen und Buchbeiträge erschienen.

Dr. Frank Imhoff ist technischer Direktor und Senior Consultant der ComConsult Beratung und Planung GmbH. Er blickt auf jahrelange Erfahrung in Forschung, Entwicklung und Betrieb von lokalen Netzen, Voice-over-IP, Wireless Local Area Networks sowie anderen Mobilfunk- und Telekommunikationssystemen zurück. Zu diesen Themenbereichen sind von ihm bereits zahlreiche Veröffentlichungen erschienen und Seminare betreut worden.

Nun folgen die wirtschaftlichen Aspekte dieser Lösungsansätze. Dabei werden sowohl die erforderlichen Investitionen für Hard- und Software (Capital Expenditure, Capex) als auch die Betriebskosten (Operational Expenditure, Opex) einer Lösung zugrunde gelegt.

Zur Ermittlung der je nach Lösungsansatz erforderlichen Investitionen wurden nach Möglichkeit die aktuellen Listenpreise der Hersteller zugrunde gelegt, die trotz aller Rabatt-Schlachten erfahrungsgemäß einen soliden Richtwert bieten. Darüber hinaus konnte jedoch auch auf die Ergebnisse von zahlreichen Ausschreibungen und einschlägigen Erfahrungen aus vielen Projekten zurückgegriffen werden. Einzig bei Microsoft liegen für die definierten Szenarien derzeit noch keine verwertbaren Erfahrungen vor, da Microsoft bei keinem der hier zugrunde gelegten Szenarien überhaupt mitgeboten hat. Zudem liegen die maßgeblichen Preise für Software-Lizenzen auch von bilateralen Vereinbarungen zwischen Microsoft und dem Kunden bzw. von den Lizenzprogrammen ab. Microsoft ist nach wie vor bestrebt, seinen Office Communications Server 2007 im Markt zu platzieren und bietet daher teilweise entsprechend niedrige (und marktferne) Projektpreise. Es bleibt also zunächst nichts anderes übrig als generell Listenpreise anzusetzen. Darüber hinaus wurde ein Wechselkurs von 1,35 USD zu einem Euro angesetzt und einige Preise im Rahmen von Webrecherchen oder Schätzungen ermittelt.

Unabhängig vom Typ und Einsatzzweck fallen für den Betrieb einer Lösungskomponente Kosten in den Kategorien Infrastruktur und Dienstleistung an. Diese Infrastruktur- und Support-Kosten entstehen letztlich sowohl für Server und Netzwerk-

## MS Office Communications Server: Total Cost of Ownership im Vergleich zu klassischen UC-Lösungen - Teil 2

komponenten in einem Rechenzentrum als auch für Endgeräte auf den Schreibtischen der Mitarbeiter und müssen daher für alle Lösungen separat kalkuliert werden. Dazu gehören z.B. folgende Punkte:

- Stellfläche
- Netzwerk-Anbindung
- Strom, Kühlung
- Grundlegende Betriebsüberwachung (Monitoring, Reporting, Statistik, Status etc.)

Bei den Dienstleistungen tragen u.a. folgende Posten zu den Kosten bei:

- Hardware-Wartung (Austausch von Geräten, Netzteilen, Lüftern, Festplatten etc.)
- Software-Wartung (Einspielen von Software-Patches, Konfigurationsänderungen etc.)
- Backup und Restore

Um die Komplexität des Betriebskostenmodells in einem überschaubaren Rahmen zu halten, wurden die oben genannten Kosten nicht einzeln für jede Lösungs-Komponente festgelegt. Stattdessen wurden verschiedene Betriebskosten-Klassen definiert. Hier wird nur grob zwischen Standard-Servern, Appliances und Endgeräten unterschieden. Dazu wurden folgende Annahmen getroffen:

- Kosten für Strom, Wartung und Support von Servern und Appliances wurde für alle Hersteller einheitlich festgelegt. Unterschiede in den Betriebskosten entstehen somit ausschließlich durch verschiedene Architekturen bzw. Komponentenmengen.

- Stromkosten wurden einheitlich mit 0,15 Euro pro Kilowattstunde angesetzt.

- Kosten für Software-Wartung wurden nicht betrachtet.

Die Betriebskosten für Standard-Server hängen u.a. von der Qualität der Infrastruktur im Sinne einer Redundanz der Strom- und Internetanbindung, der Sicherheitsreserven bei der Kühlung sowie der Vorkehrungen gegen Brände usw. ab. Unternehmen in den hier betrachteten Größenordnungen verfolgen in diesem Zusammenhang in der Regel hohe Standards, vor allem vor dem Hintergrund der großen Bedeutung der Telefonie. Das gleiche gilt für Dienstleistungen für die vor allem bei einer externen Vergabe der Aufgaben Service Level Agreement (SLA) definiert werden. Diese unterscheiden sich deutlich hinsichtlich des Umfangs, der Betriebs-, Service- und Reaktionszeiten, jedoch werden bei zentralen TK-Komponenten immer die allerhöchsten Maßstäbe angelegt. Aus diesen Gründen wurde den Wartungs- und Supportkosten der Server-Klassen die Preise (ca. 250 Euro) renommierter Housing- bzw. Hosting-Anbieter zugrunde gelegt. Bei Servern, die an abgesetzten Standorten mit weniger als 100 Mitarbeitern installiert sind, wurden deutlich erhöhte Wartungspauschalen angesetzt (ca. 350 Euro), da hier ein höherer Aufwand aufgrund der Anreise von Servicetechnikern etc. üblich ist.

Im Vergleich zu Standard-Servern zeichnen sich die hier definierten Appliances durch eine größere Vielfalt, typischerweise geringeren Stromverbrauch, weniger Konfigurationsänderungen und geschlossene Systeme aus. Aus den letzten beiden Punkten ergibt sich u.a. ein geringerer Aufwand beim Backup und ein einfacherer Support, da in der Regel keine Reparaturen sondern nur ein Austausch der Geräte stattfindet. Zu den Appliances gehören aber z.B. auch PSTN-Gateways, ATAs oder IP-DECT Basisstationen. Um der Vielfalt gerecht zu werden ist neben der Unterscheidung zwischen zentral und remote installierten Geräten auch eine Unterteilung nach der „Größe“ der Geräte statt, wobei die Einteilung vom Stromverbrauch und dem Preis der Appliance abhängig ist. Dementsprechend reichen die zugrunde gelegten monatlichen Wartungs- und Supportkosten für Appliances von 1 bis zu 300 Euro sowie der der Stromverbrauch von 10 bis 2000 Watt.

**Endgeräte**

Bei den Endgeräten müssen Basis-, Standard-, Comfort-Geräten und Softphones unterschieden werden. In deren Betriebskosten fließen sowohl die Stromkosten als auch die Wartungs- und Supportkosten ein. Die Stromkosten basieren dabei auf Herstellerangaben für die verwendeten Geräte. Der üblicherweise verwendete Wert für den On-Hook-Status ist jedoch nicht hinreichend aussagekräftig. Ein typisches Arbeitsplatztelefon wird schließlich nur während der Arbeitszeit benötigt und ist damit zwei Drittel des Tages ohne Funktion. Über das Jahr betrachtet liegt der Anteil der „unproduktiven“ Zeit sogar bei rund 80% wenn man Wochenenden, Urlaub, Krankheitstage etc. hinzuzählt. Aus diesem Grund ist der Strombedarf eines Geräts im Standby-Modus – sofern das Gerät über einen solchen Modus verfügt – von besonders großer Bedeutung.

Um den „typischen“ Stromverbrauch eines Endgerätes zu ermitteln, wurde daher ein einfaches Rechenmodell verwendet, das mit den Herstellerwerten parametrisiert wurde. Die Werte für die unterschiedlichen Modi (on-hook, active, ringing und standby) wurden den jeweiligen Datenblättern der Hersteller entnommen bzw. im ComConsult Test-Center gemessen. Die Kosten für Wartung und Support ergeben sich aus marktüblichen Portpreisen, wobei der Anteil des Anschaffungspreises für das Endgerät herausgerechnet wurde. Diese sind schließlich in den Investitionskosten enthalten. Es wird davon ausge-

MS Office Communications Server: Total Cost of Ownership im Vergleich zu klassischen UC-Lösungen - Teil 2

gangen, dass sich die Hersteller in dieser Beziehung nicht unterscheiden, d.h. die Wartungskosten sind über alle Hersteller identisch. Damit ergibt sich für Endgeräte ein Leistungsbedarf zwischen 0 Watt für Softphones (ohne Headset), 3,0 Watt für Standard-Endgeräte von SEN und 7,1 Watt für Comfort-Endgeräte von Cisco. Der Wartungsaufwand wurde je nach Geräteklasse mit Kosten zwischen 0,10 Euro und 2,00 Euro angesetzt. Bei Microsoft werden aufgrund der fehlenden Auswahl an Endgeräten die Klassen Comfort und Standard zusammengelegt.

**Investitionen**

Unabhängig vom betrachteten Szenario wird deutlich, das Microsoft derzeit keine technische und wirtschaftliche Alternative zu einer echten TK-Lösung darstellt. Je stärker ein Unternehmen verteilt ist und je kleiner die einzelnen Standorte desto unwirtschaftlicher wird ein OCS-basierter Lösungsansatz. Besonders deutlich wird dies bei Szenario 1 (Einzelhandelskette, Abbildung 1), wo der Invest für die Microsoft-Lösung beim doppelten der SEN-Lösung liegt. Hier übersteigen allein die Hardware-Kosten die vollständigen Investitionskosten der SEN-Lösung. Da kein zentrales Bereitstellen der OCS Funktionalität in Rechenzentren vorgesehen ist, muss – auch aus Gründen der Survivability – an jedem noch so kleinen Standort ein ähnlicher Aufwand betrieben werden, wie in den Rechenzentren. Gemäß den Planungswerkzeugen von Microsoft, ist in einem Standort mit 100 Nutzern die Installation von mindestens einem Frontend Server, einem Edge Server und einem Mediation Server notwendig. Wird Redundanz verlangt verdoppelt sich die Anzahl der Server. Hinzu kommen IIS, SQL und Reverse Proxy sowie im Falle von redundanten Kernkomponenten mindestens zwei Loadbalancer für internen und externen Zugriff. Damit ergibt sich ein Bedarf von mindestens neun Servern zuzüglich Gateways und Loadbalancer für einen Standort von gerade einmal 100 Mitarbeitern.

Da dies den Planungshinweisen Microsofts entspricht, wurde diese Architektur hier zugrundegelegt. Es sei jedoch ausdrücklich darauf hingewiesen, dass – je nach individuellem Kommunikationsaufkommen in den einzelnen Standorten - dieser Aufbau konsolidiert werden kann. Eine Möglichkeit liegt in der konsolidierten Installation der verschiedenen Serverrollen des OCS auf einer Hardware. Lediglich der Mediation Server verlangt die alleinige Installation. Zudem könnten Webserver und Datenbank auf einer Plattform zusammengelegt werden. CDR/Archiving Server sind an den einzelnen Standorten nicht notwendig. In Bezug auf den Mediation Server besteht ebenfalls Optimierungspotential. So könnten Gateways zum Einsatz kommen, welche bereits einen OCS Mediation Server beinhalten und mittlerweile von mehreren Herstellern verfügbar sind. Bei geringer Last könnte darüber hinaus eine Virtualisierung der verschiedenen Server in Betracht gezogen werden, womit durch zwei „echte“ Server zuzüglich Gateways bereits eine redundante Lösung implementiert werden könnte. Diese Methode zur Reduzierung der Hardwarekosten werden von Microsoft jedoch nicht unterstützt, so dass der Kunde bei Problemen auf sich allein gestellt ist.

Die Kostennachteile der Microsoft-Lösung lassen sich jedoch nur im Filial-Szenario derart deutlich aus den Zahlen ableiten. Immerhin sind die Investitionskosten in allen anderen Vergleichen annähernd vergleichbar und in einigen Fällen sogar niedriger als bei anderen Herstellern (siehe Abbildung 2 und Abbildung 3). Vor allem im Szenario des Chemieunternehmens bestanden hohe Anforderungen an die Integration von konventioneller Technik. Der OCS erfordert hierzu hybride Systeme von anderen Herstellern. Dies können Bestandsanlagen sein oder neu beschaffte Systeme. Zugunsten von Microsoft wurde in den Szenarien 2 und 3 davon ausgegangen, dass die Bestandsanlagen weiter betrieben werden. Dies verschleiert jedoch, dass die Lösung auf Altsystemen aufbaut, für die keine Ersatzteile und keine Wartung mehr verfügbar sind. Hier zeigt sich der Fokus der Microsoft-Lösung auf Büroumgebungen – in den meisten Unternehmen kann der OCS daher nur Teil einer Gesamtlösung sein.

Interessanter ist der Vergleich für die Lösungen von Cisco und SEN, da die Produkte technisch vergleichbar sind. Bei den Investitionen ist die SEN-Lösung in al-

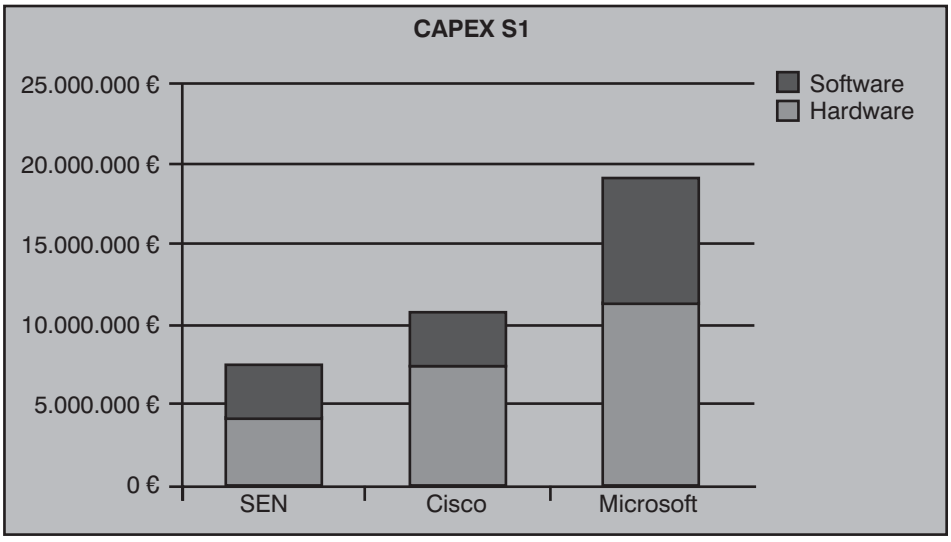



Abbildung 1: Vergleich der Investitionen (CAPEX) für Szenario 1 (Filialunternehmen)

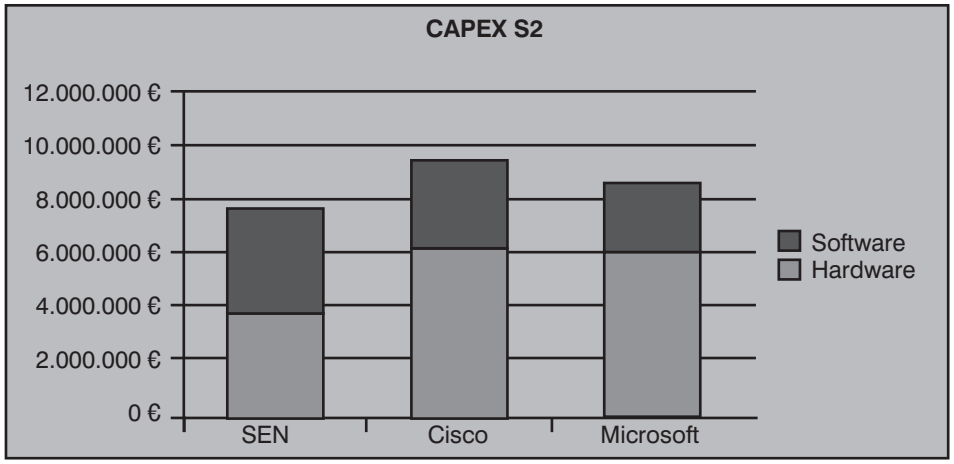



Abbildung 2: Vergleich des CAPEX für Szenario 2 (Dienstleistungsunternehmen)

MS Office Communications Server: Total Cost of Ownership im Vergleich zu klassischen UC-Lösungen - Teil 2

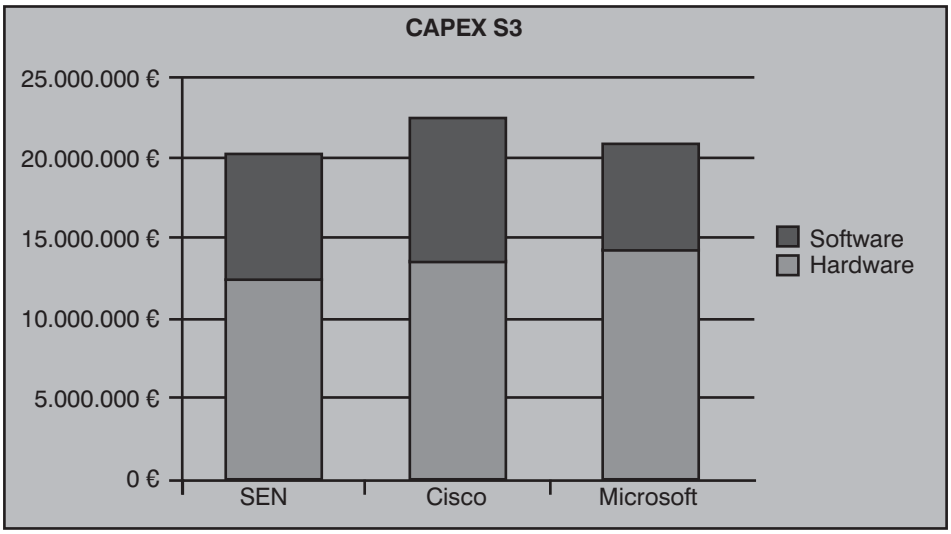



Abbildung 3: Vergleich des CAPEX für das Szenario 3 (Chemiekonzern)

len hier betrachteten Fällen günstiger als Cisco. Grundsätzlich wird dies durch die Ergebnisse zahlreicher Ausschreibungen bestätigt. Dennoch sind die Unterschiede nicht hinreichend signifikant, um dieses Ergebnis zu verallgemeinern. Neben Rabatten, Trade-In-Optionen und anderen durch das Modell unberücksichtigten Aspekten stellen sich in der Praxis auch viele technische Details als preisbildend heraus. So wird beispielsweise die ab Werk durch den Cisco Communications Manager unterstützte Chef-Sekretär-Funktion häufig als funktional unzureichend empfunden – Abhilfe schaffen hier nur Software-Lösungen von Cisco-Partnern. Andererseits bieten z.B. Ciscos SRST-Router deutlich mehr Funktionalität als die Survivability-Gateways von SEN. Hier können also bei SEN-Kunden noch deutliche Mehrkosten entstehen.

Trotz der ähnlich hohen Investitionskosten lässt die Kostenverteilung Unterschiede erkennen. Bei SEN wirkt sich vor allem der hohe Preis für Benutzerlizenzen negativ auf den CAPEX aus, während bei Cisco die zentralen Komponenten und SRST-Router in den Außenstellen stark zu den Gesamtkosten beitragen.

### Betriebskosten

Bei den laufenden Kosten schlagen die bei Microsoft fehlenden Lösungen für Außenstellen heftig zu, denn dort muss derzeit noch mit großen Hardware-Mengen gerechnet werden. Im stark verteilten Szenario 1 liegen die monatlichen Kosten für den Betrieb der SEN- und Cisco-Lösung beispielsweise bei rund 184.000 Euro bzw. 192.000 Euro – die Aufwendungen für die Microsoft-Lösung betragen ca. das Achtfache dessen. In den anderen Szenarien liegen die Betriebskosten immerhin beim drei- bis vierfachen der beiden anderen Hersteller. Diese enormen laufenden Ausgaben schlagen sich selbstverständlich deutlich im TCO nieder, wie in nachfolgenden Abschnitten zu sehen sein wird. Lediglich bei den Betriebskosten für Endgeräte kann Microsoft punkten, wenn viele Mitarbeiter mit Softphones ausgestattet werden können. Dem Modell folgend lassen sich für diesen Teilbereich die Kosten durch den flächendeckenden Einsatz von Softphones um mehr als ein Viertel senken. Dieses Planspiel würde jedoch bei anderen Herstellern in etwa zum selben Ergebnis führen.

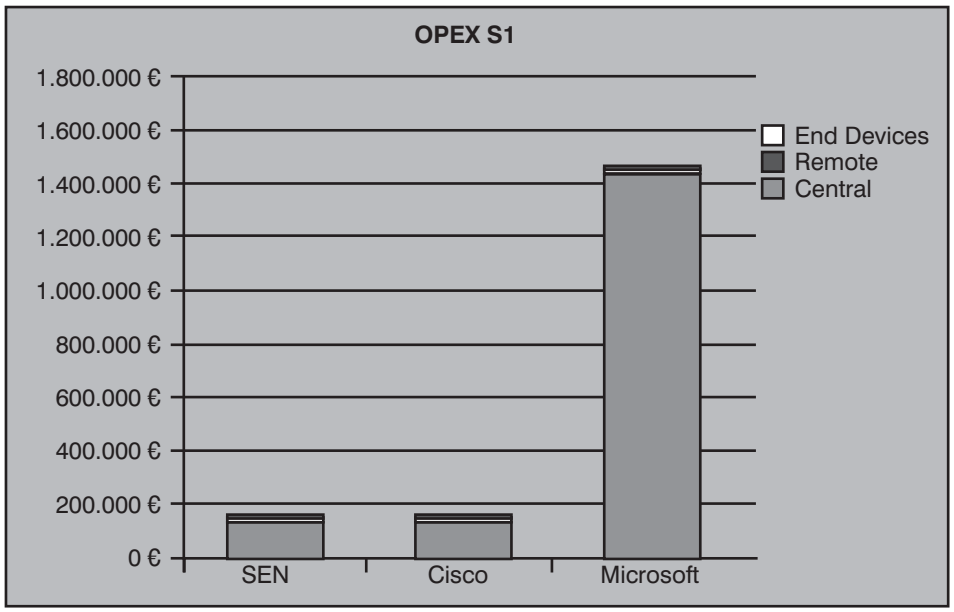



Abbildung 4: Vergleich der Betriebskosten für das Szenario 1 (Filialunternehmen)

Der Vergleich der Betriebskosten von SEN und Cisco fällt auf den ersten Blick uneindeutig aus. Im ersten Szenario besteht praktisch ein Gleichstand, beim zweiten Szenario ist die SEN-Lösung etwas günstiger und beim dritten Szenario zeigen sich Vorteile für Cisco. Die Unterschiede sind weit weniger deutlich als im Vergleich zu Microsoft, können jedoch bei TCO-Betrachtungen über einige Jahre hinweg ausschlaggebend bei der Bewertung der Wirtschaftlichkeit sein. Bezüglich des letzten Szenarios ist zudem anzumerken, dass die SEN-Lösung die Bestandsanlagen durch HiPath 4000 Systeme ablöst, deren laufende Kosten Teil des OPEX sind. Bei der Cisco-Lösung bleiben die Bestandsanlagen hingegen bestehen.

Bei der Struktur der Betriebskosten ergeben sich deutliche Unterschiede zwischen Cisco und SEN. Bei SEN wirkt sich der Mangel an PSTN-/Analog-Gateways mit integrierten SIP-Proxies für Zweigstellen, in einigen Fällen negativ aus. Mehrere Einzelkomponenten erzeugen einen höheren Betriebsaufwand als ein integriertes Gerät. Hingegen liegen die Kosten für den Betrieb der zentralen Komponenten bei Cisco in fast allen Szenarien deutlich über den Kosten der SEN-Lösung – im Fall des Filialunternehmens sogar um mehr als das Doppelte. Bei den Betriebskosten der Endgeräte ist die SEN-Lösung durch den niedrigeren Stromverbrauch ebenfalls leicht im Vorteil.

### Stromverbrauch

Unabhängig vom Hersteller ist der Anteil der Stromkosten an den Betriebskosten einer Lösung abhängig vom Verteilungs-

## MS Office Communications Server: Total Cost of Ownership im Vergleich zu klassischen UC-Lösungen - Teil 2

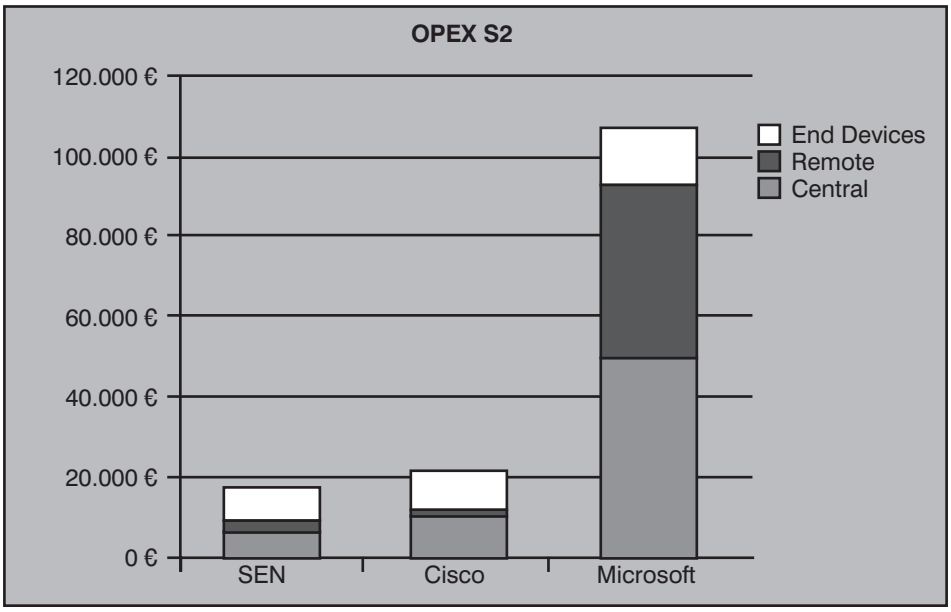



Abbildung 5: Vergleich der Betriebskosten für Szenario 2 (Dienstleistungsunternehmen)

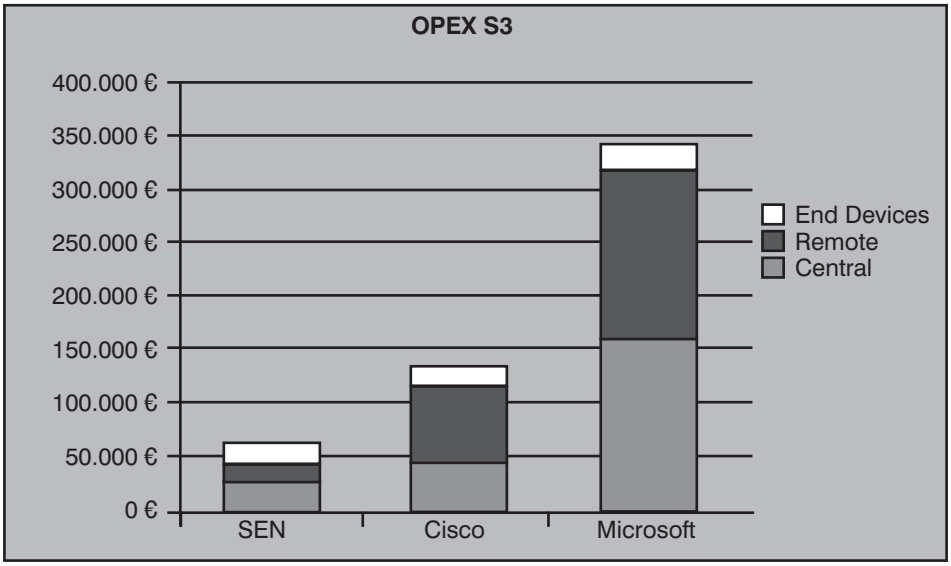



Abbildung 6: Vergleich der Betriebskosten für Szenario 3 (Chemiekonzern)

grad des Kundenszenarios. Bei stark verteilten Szenarien (z.B. beim Filialunternehmen) liegt der Anteil bei allen Herstellern bei rund 10%. Bei anderen Szenarien schwankt der Anteil bei SEN und Cisco je nach Zentralisierungsgrad zwischen einem Viertel und einem Drittel der Betriebskosten. Lediglich bei Microsoft werden die Betriebskosten aufgrund des hohen Hardware-Aufwands in den Außenstandorten von den Wartungs- und Supportkosten dominiert. Es ist somit offensichtlich, dass der Stromverbrauch insbesondere bei zentralisierten Kundenszenarien einen signifikanten Teil zu den Betriebskosten beiträgt. In allen betrachteten Szenarien liegt SEN bei der Energieeffizienz vor den anderen Herstellern. Abhängig vom Szenario sind hier Einsparungen von mehreren Tausend Euro pro Monat im Vergleich zu den Konkurrenzlösungen möglich.

Betrachtet man die Verteilung des Stromverbrauchs über die verschiedenen Lösungskomponenten hinweg, so werden wieder architektonische Unterschiede deutlich (siehe Abbildung 7). Grundsätzlich spielt SEN seine Stärken bei den zentralen Komponenten, d.h. insbesondere bei der HiPath 8000 sowie bei den Endgeräten aus. Der Anteil von Servern und Endgeräten am Stromverbrauch ist bei SEN maximal 65% während dieser Wert bei Cisco 83% und bei Microsoft sogar 91% betragen kann. Die Stärke von Cisco sind die integrierten Router für Außenstellen. Aufgrund der höheren Integrationsdichte zeigen sich hier Vorteile bei der Energieeffizienz. Microsoft hingegen scheint beim Verbrauch der Endgeräte Vorteile zu besitzen, jedoch ist dies nur ein Effekt der gelockerten Anforderungen an die Microsoft-Lösung. Da mit dem Tanjay letztlich nur ein Hardphone für den OCS zur Verfügung steht, benutzt die Masse der Teilnehmer ein Softphone mit USB-Headset. Dass sich hieraus Vorteile beim Energieverbrauch ergeben, liegt auf der Hand. Die guten Werte der Microsoft-Lösung bei den Endgeräte-Stromkosten weisen daher allgemein auf die kostentechnischen Vorteile von Softphones hin.

Lässt man Microsoft außen vor und vergleicht lediglich SEN und Cisco bezüglich der Energieeffizienz ihrer Endgeräte, so zeigen sich Unterschiede. Quer durch alle Szenarien liegen die Stromkosten der Siemens-Geräte im Vergleich zu entsprechend ausgestatteten um rund 30% unter vergleichbaren Hardphones von Cisco. Dies ist vor allem dem Standby-Modus der OpenStage-Geräte zuzuschreiben, der den Verbrauch über ein Jahr betrachtet erheblich reduziert. Aber auch im Ge-

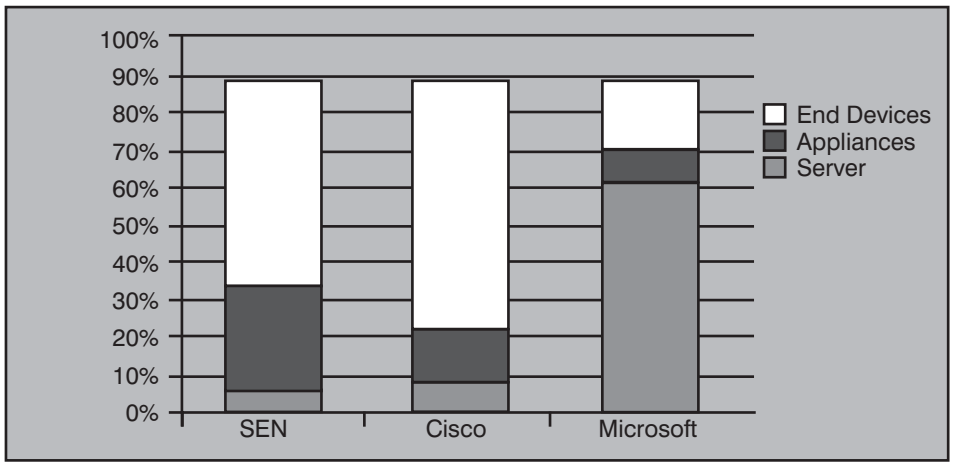



Abbildung 7: Anteile der Lösungskomponenten am Stromverbrauch für Szenario 3

spräch (Active-Modus) bzw. im normalen Betriebsmodus (On-Hook) liegt der Verbrauch stets unter den Vergleichsgeräten von Cisco. Abbildung 8 vergleicht die Geräte der drei Kategorien in den verschiedenen Modi.

Der Effekt des Standby-Modus zeigt sich besonders deutlich bei den Endgeräten der Comfort-Klasse. Der für typische Büroumgebungen kostenbestimmende Standby-Modus des OpenStage 60 reduziert den Verbrauch von 6,9 Watt (On-Hook) auf 3,3 Watt (Standby). Das Cisco 7965G verfügt zwar auch über einen Standby-Modus, jedoch ist der Effekt hier mit 0,4 Watt Minderverbrauch deutlich geringer. Es ist damit zu rechnen, dass Cisco und andere Hersteller bald nachziehen und verbrauchsoptimierte Endgeräte anbieten.

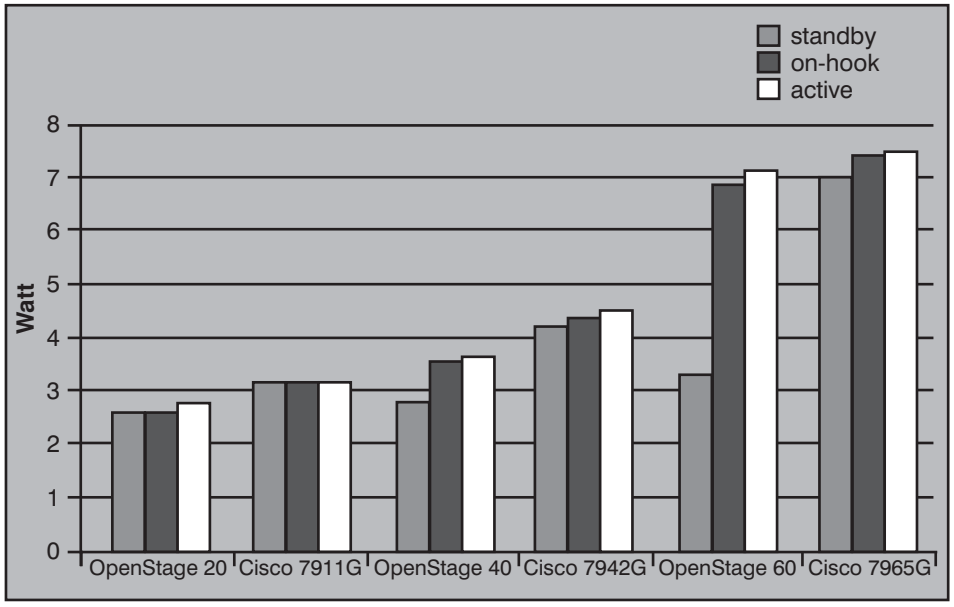



Abbildung 8: Vergleich des Stromverbrauchs von Cisco- und SEN-Telefonen

### Total Costs of Ownership

Betrachtet man den TCO auf 36 bzw. 60 Monate, so zeichnen sich aufgrund der beschriebenen Kostenstrukturen Vorteile für die SEN-Lösung ab. Die negativen Ergebnisse bezüglich der Investitions- und Betriebskosten des Microsoft OCS schlagen sich selbstverständlich auch auf den TCO-Vergleich nieder. Trotz der z.T. deutlichen Zugeständnisse an die technischen Unzulänglichkeiten des OCS ist dieser auch bezüglich des TCO nicht konkurrenzfähig. Im besten Fall (Szenario 2) liegen die Kosten auf drei Jahre gerechnet rund 9% über der SEN-Variante. Dieser annähernde wirtschaftliche Gleichstand wird jedoch mit dem Weiterbetrieb der veralteten Bestandsanlage und allen damit verbundenen Risiken und Problemen erkauft. Sollte das veraltete TK-System 60 Monate ohne Probleme überstehen, dann liegt der TCO der Microsoft-Lösung in diesem Szenario dennoch um rund ein Viertel über dem der SEN-Lösung. Der Kunde hätte mit dieser riskanten Lösungsvariante nichts gewonnen.

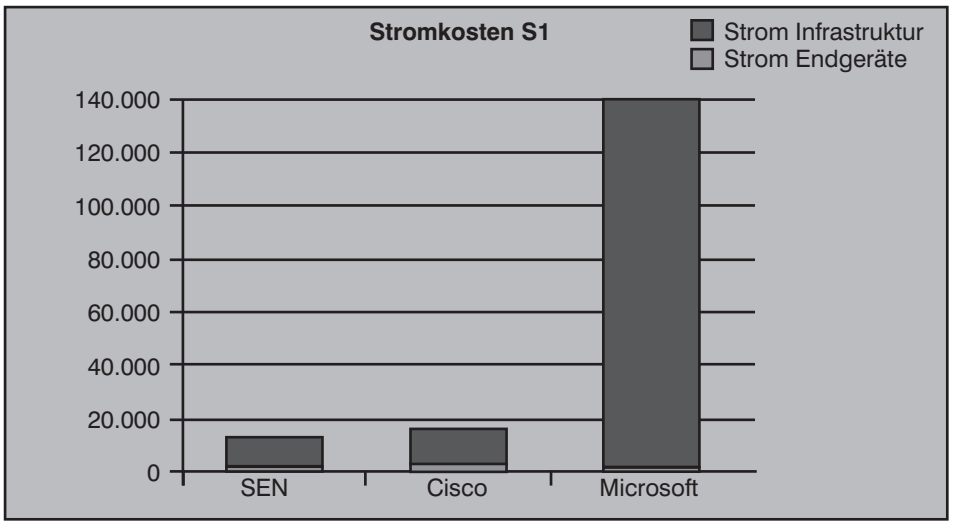



Abbildung 9: Vergleich der Stromkosten für das Szenario 1 (Filialunternehmen)

Im Vergleich zu Cisco schneiden die TCO von SEN in der Regel besser ab. Eine Analyse der Faktoren zeigt, dass die SEN-Lösung vor allem bei den Nutzer-Lizenzen und bei den Endgeräten kostenintensiver ist als die entsprechenden Cisco-Komponenten. Auf der anderen Seite wirken sich vor allem die niedrigeren Kosten für periphere Hardware sowie für Hardware, Software und Lizenzen von UC-Applikationen positiv auf den TCO der SEN-Lösung aus.

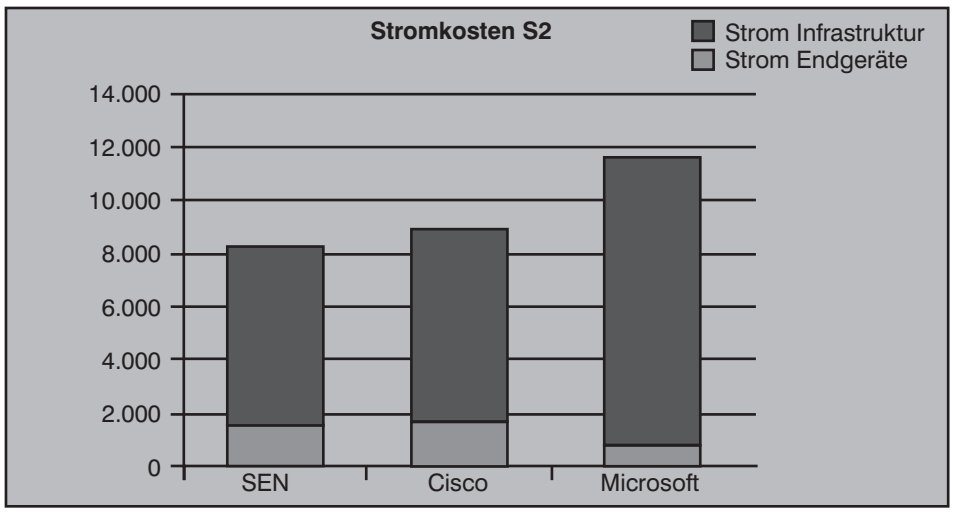



Abbildung 10: Vergleich der Stromkosten für das Szenario 2 (Dienstleistungsunternehmen)

Es muss betont werden, dass die Betriebskosten in der Praxis einen größeren Einfluss auf die TCO besitzen als von den vorliegenden Modellrechnungen sugge-

MS Office Communications Server: Total Cost of Ownership im Vergleich zu klassischen UC-Lösungen - Teil 2

riert. Während den Betriebskosten realistische Werte zugrunde liegen sind die Investitionskosten durch die Verwendung von Listenpreisen stark überhöht. Projektpreise für Unternehmen in den betrachteten Größenordnungen liegen deutlich unter den offiziellen Preisangaben der Unternehmen. Nachlässe von 50% und mehr sind keine Seltenheit.

**Fazit**

Der hier vorliegende Vergleich der TCO zeigt deutlich, dass Microsoft auch bei sehr großzügiger Interpretation der Anforderungen und unter Vernachlässigung einiger Kostenaspekte kaum mit „klassischen“ TK-Herstellern Schritt halten kann. Unter den hier gegenübergestellten Lösungen schneidet SEN als traditionell am meisten von TK geprägter Hersteller sehr gut ab. In allen hier betrachteten Szenarien ist die SEN-Lösung unter Kostenaspekten bei gleichen Anforderungen mindestens genauso wirtschaftlich wie der Mitbewerb.

Microsoft wird das wenig grämen, denn schließlich ist in regelmäßigen Beteuerungen immer wieder zu hören, dass Microsoft (noch) keine TK-Lösung anbietet. Insofern werden hier also aus Sicht von Microsoft Äpfel mit Birnen verglichen. Aber selbst unter Vernachlässigung des für Microsoft sehr ungünstigen Filial-Szenarios liegen die TCO des OCS deutlich über denen der SEN-Lösung. Hauptgrund sind die eingeschränkten Möglichkeiten zur Zentralisierung des OCS und die daraus resultierenden Betriebskosten. Zudem erfordert jedes realistische Szenario zusätzliche TK-Anlagen, zumindest um konventionelle Geräte wie Aufzugtelefone oder Faxgeräte anzubinden und die immer noch unverzichtbare Chef-Sekretär-Funktionalität zu bieten. Das gilt auch für OCS R2. Diese Version bringt zwar wichtige Verbesserungen mit sich, jedoch bleiben die grundlegenden Mängel der OCS-Architektur vorerst erhalten.

Bis zum dritten Release des OCS, das vermutlich 2010 erscheinen wird, stellt die Microsoft-Lösung bei einer reinen TCO-Betrachtung keine ernstzunehmende Alternative für UC-Lösungen klassischer TK-Hersteller – und dazu zählt hier auch Cisco – dar. Erst dann, wenn funktionale Vorteile einer OCS-Lösung zum Tragen kommen, können sich hier natürlich andere Ergebnisse konstatieren.

Der Vergleich zwischen SEN und Cisco fällt nicht so eindeutig aus. Bei den Investitionen zeigen sich leichte Vorteile für SEN, die jedoch erfahrungsgemäß

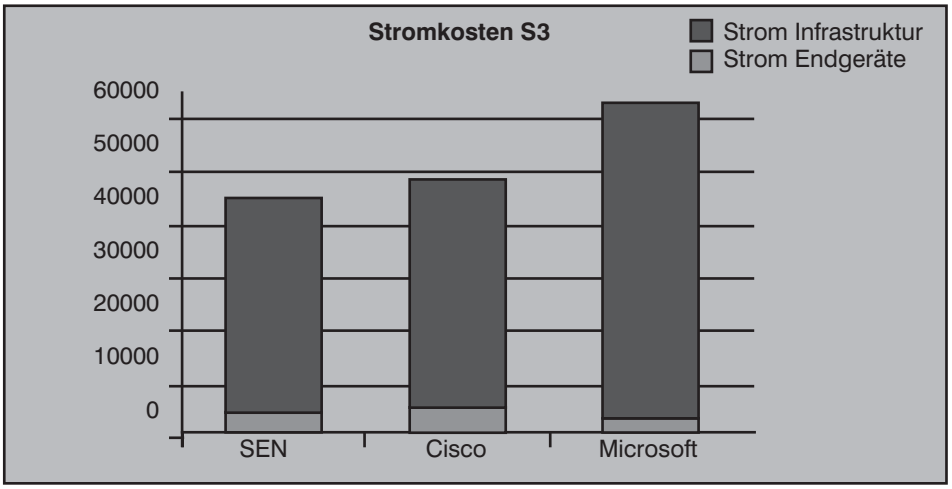



Abbildung 11: Vergleich der Stromkosten für das Szenario 3 (Chemiekonzern)

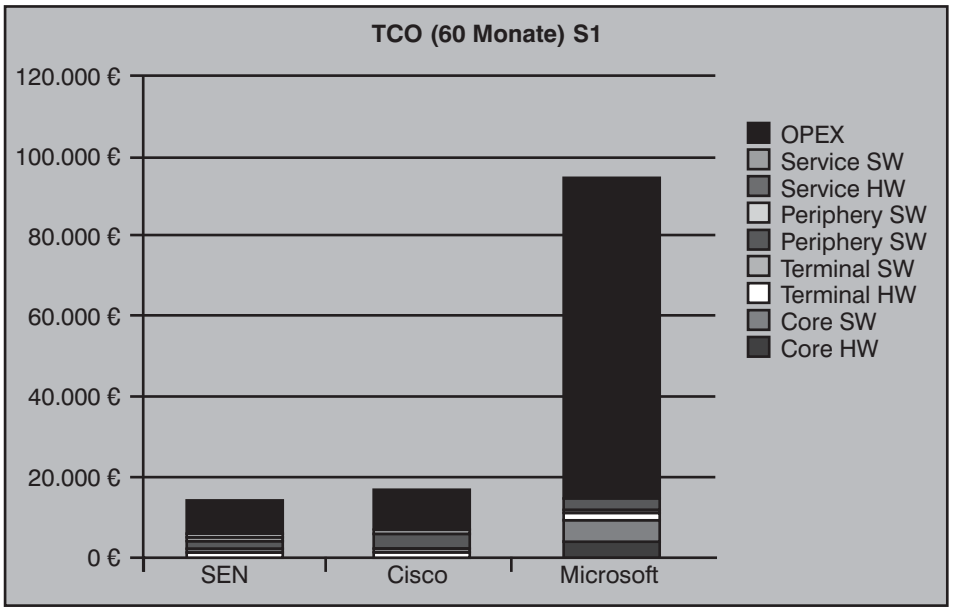



Abbildung 12: TCO nach 60 Monaten für das Szenario 1 (Filialunternehmen)

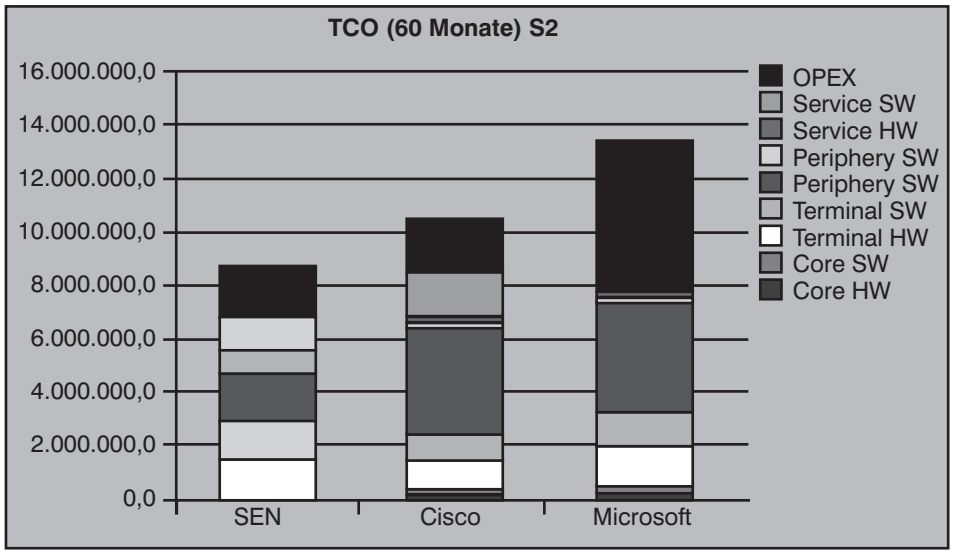



Abbildung 13: TCO nach 60 Monaten für das Szenario 2 (Dienstleistungsunternehmen)

## MS Office Communications Server: Total Cost of Ownership im Vergleich zu klassischen UC-Lösungen - Teil 2

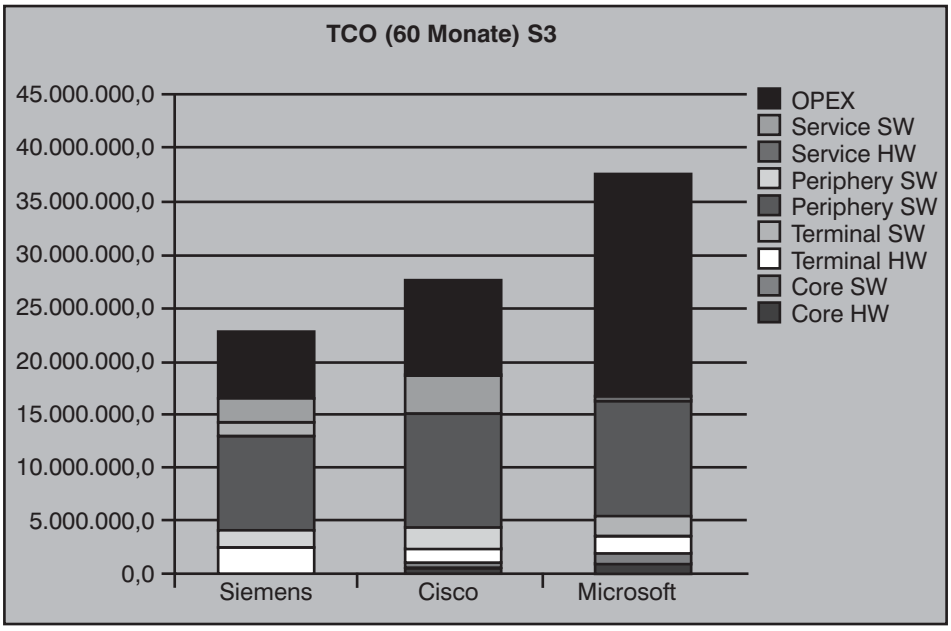



Abbildung 14: TCO nach 60 Monaten für das Szenario 3 (Chemiekonzern)

im Rahmen der Verhandlungsspannen liegen und zudem vom Dollarkurs abhängen. Deutlich wird jedoch, dass die SEN-Lösung im Bereich der UC-Applikationen erhebliche Kostenvorteile zeigt. Auch bei den Betriebskosten spielen die SEN-Produkte aufgrund der zentralen Komponenten sowie des geringeren Stromverbrauchs der Endgeräte ihre Stärken aus. Hinzu kommt, dass vor allem bei Industriekunden häufig konventionelle Technik in eine neue VoIP-Infrastruktur integriert werden muss. Dies ist mit SEN sowohl in technischer als auch in wirtschaftlicher Hinsicht leichter zu bewerkstelligen.

Bei all diesen Vergleichen darf jedoch eines nicht vergessen werden: Neben den Kosten ist die Funktionalität und Benutzerfreundlichkeit einer Lösung sicherlich von erheblicher Bedeutung. Und in diesem Punkt unterscheiden sich die hier verglichenen Lösungen z.T. erheblich. Gerade mithilfe des noch vergleichsweise jungen Unified-Communications-Themas sind in den allermeisten Unternehmen noch erhebliche Effizienz-Steigerungen zu erwarten. Damit lassen sich zweifelsohne unvergleichbar größere Kosteneinsparungen und Wertschöpfungspotenziale erzielen als durch reduzierte Energiekosten aufgrund von Standby-Funktionen oder eine etwas kleinere Serverfarm. Die voranschreitende Virtualisierung wird einiges dazu beitragen.

Es reicht also bei weitem nicht, die erforderlichen Betriebskosten und Investitionen einer Lösung zu addieren. Vielmehr müssen weiter entfernt liegende Einsparpotenziale umfassend evaluiert und in die Kalkulation einbezogen werden. Wenn sich beispielsweise 10.000 Mitarbeiter an die im Vergleich zu einem herkömmlichen Telefon gänzlich neue Oberfläche eines Softphones oder Kollaborationsplattformen gewöhnen müssen, sind immense Kosten zu erwarten. Auf der anderen Seite lassen sich dadurch aber möglicherweise Arbeitsschritte erheblich vereinfachen, die Zusammenarbeit zwischen weit entfernt oder verteilt arbeitenden Teams verbessern und vieles andere mehr. Wenn dadurch dann Dienstreisen und Doppelarbeit vermieden wird, dürfen geringfügig höhere Investitionen und gar Stromkosten nicht im Weg stehen.

Ein weiterer Aspekt und wesentlicher Bestandteil von UC ist die Applikationsintegration. Ein Hersteller, der aufgrund seiner Marktpräsenz und seiner inzwischen jahrzehntelangen Erfahrung mit der Entwicklung von Software hat, ist hier zweifelsohne im Vorteil. Es ist nicht zu übersehen, dass die zunehmende Integration sowohl die Investitions- als auch die Betriebskosten erhöhen. Nur die Hersteller von UC-Lösungen, deren Produkte sich mit möglichst vielen Applikationen nahtlos und kosteneffektiv verbinden lassen, können hier dauerhaft punkten. Es ist heute noch nicht sicher, wer das sein wird. Klar ist aber, dass die klassischen TK-Hersteller es schwer haben werden.

Sonderveranstaltung

# Ausschreibungen im Informations- und Kommunikationsbereich

## Leitfaden für öffentliche Auftraggeber

**Die ComConsult Akademie veranstaltet vom 18.06.09 ihre Sonderveranstaltung „Ausschreibungen im Informations- und Kommunikationsbereich“ in Bonn.**

Die Neuerungen des Vergaberechts stellen öffentliche Auftraggeber, die Leistungen im Informations- und Kommunikationsbereich ausschreiben, vor neue Herausforderungen. Unter den Bedingungen verschärfter gesetzlicher Auflagen muss die öffentliche Hand im hochkomplexen Bereich der Informations- und Kommunikationstechnologie oft unter großem Zeitdruck Vergabeverfahren durchführen. Hier ist interdisziplinäre Kompetenz dringend vonnöten. Um Risiken im Vergabeverfahren zu vermeiden, sind die öffentlichen Auftraggeber auf juristische Expertise angewiesen. Um die technischen Ziele im IT- und Kommunikationsbereich (ITK) zu erreichen, brauchen die ausschreibenden Stellen erfahrene Planer, die jahrelange Ausschreibungspraxis mitbringen.

Diese kombinierte Expertise ist genau das, was Ihnen die eintägige Sonderveranstaltung der ComConsult Akademie zu Ausschreibungen im Informations- und Kommunikationsbereich bietet. Diese Veranstaltung ist als Leitfaden für öffentliche


Auftraggeber gedacht, die in ihren ITK-Vergabeverfahren unter Einhaltung aller gesetzlichen Auflagen und Vermeidung aller rechtlichen Risiken für ihre Verwaltung das optimale Ausschreibungsergebnis erreichen wollen. Planer mit jahrzehntelanger Erfahrung bei Ausschreibungen der öffentlichen Hand vermitteln auf dieser Veranstaltung ihren Erfahrungsschatz. Das juristische Wissen wird von einem renommierten Rechtsanwalt mit dem Spezialgebiet Vergaberecht präsentiert.

Die Sonderveranstaltung beantwortet die folgenden Fragen:

- Was sind die Neuerungen des Vergaberechts und welche Relevanz haben sie für die Ausschreibungen?
- Was ist die richtige Ausschreibungsform für Projekte im Informations- und Kommunikationsumfeld?
- Welche Fallstricke sollte man auf jeden Fall vermeiden?
- Wie sind Angebote zu bewerten?
- Welche Besonderheiten sind im Bereich der Informations- und Kommunikationstechnik zu berücksichtigen?

Die Sonderveranstaltung richtet sich u.a. an Personen aus den folgenden Bereichen öffentlicher Verwaltungen:

- IT-Management
- IT-Planer
- Verantwortliche für die Telekommunikation
- Beschaffungswesen

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

Fax-Antwort an ComConsult 02408/955-399

# Anmeldung

## Ausschreibungenim Informations- und Kommunikationsbereich

Ich buche das Seminar
**Ausschreibungen im Informations- und Kommunikationsbereich**
☐ 18.06.09 in Bonn
zum Preis von 790,- € zzgl. MwSt.

☐ Bitte reservieren Sie für mich ein Hotelzimmer im Hilton Bonn

vom_____ bis_____09

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

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

Neuauflage Technologie-Report

# Wide Area Networks:
## Technik und Funktionsweise

**Soeben ist der Report „Wide Area Networks: Technik und Funktionsweise“ von Dr. Behrooz Moayeri und Dipl.-Inform. Andreas Meder erschienen.**

Moderne Datennetze werden seit Jahrzehnten hinsichtlich ihrer Reichweite wie folgt kategorisiert:

- Local Area Network (LAN): Ein solches Netz wird im Gebäude oder Gelände eines Unternehmens oder einer Organisation aufgebaut.
- Metropolitan Area Network (MAN): Ein MAN erstreckt sich in der Regel auf ein Stadtgebiet oder eine vergleichbare geografische Größe.
- Wide Area Network (WAN): Ein Weitverkehrsnetz verbindet verschiedene Standorte über große Entfernungen miteinander und kann sogar die Dimensionen des gesamten Globus annehmen.

Zu Beginn der Entwicklung moderner Datennetze wurden im LAN-Bereich unabhängig voneinander verschiedene Verfahren und Techniken entwickelt und eingeführt. In den letzten zehn Jahren wurden jedoch alle anderen LAN-Typen von Ethernet oder genauer von Netzen gemäß dem Standard IEEE 802.3 verdrängt. Heute sieht basiert ein LAN in China auf der selben Technologie wie ein LAN in Europa oder Lateinamerika.

Anders im Bereich WAN: Hier herrscht Vielfalt. Weitverkehrsnetze variieren nicht nur von Region zu Region, abhängig von


der historischen Entwicklung des Marktes in den jeweiligen Ländern, sondern innerhalb eines Landes. Zwar wird erwartet, dass Ethernet langfristig über den LAN-Bereich hinaus auch den MAN- und WAN-Markt dominieren wird, aber davon sind wir noch entfernt. Ethernet ist heute eine der im WAN-Bereich eingesetzten WAN-Technologien. Daneben gibt es noch eine große Zahl verschiedener Verfahren und Netzarchitekturen. WAN-Technologien sind besonders langlebig. Hin und wieder begegnet man sogar sehr alten Verfahren wie X.25.

Vor diesem Hintergrund stehen die Planer und Betreiber von Weitverkehrsnetzen mit dem Problem konfrontiert, die für ihre Zwecke passendste Technologie auszuwählen bzw. die Angebote der Service Provider im WAN-Bereich zu bewerten. Es kann durchaus sein, dass dem selben Unternehmen in einer Ausschreibung von verschiedenen Providern WAN-Lösungen mit völlig unterschiedlichen Technologien angeboten werden. Was ist die richtige Lösung für dieses Unternehmen? Dieser Report soll bei der Beantwortung dieser Frage helfen.

Der vorliegende Report basiert auf den jüngsten Erfahrungen von Experten mit jahrelanger Erfahrung im Bereich der Konzipierung, der Planung und dem Betrieb von WAN-Lösungen. Die Autoren kommen aus der Praxis und vermitteln dem Leser ihr Wissen über verschiedene Technologien und Netzarchitekturen im WAN-Bereich.

Die Autoren dieses Reports sind Dr.-Ing. Behrooz Moayeri und Dipl.-Inform. Andreas Meder. Herr Moayeri hat viele Großprojekte mit dem Schwerpunkt standortübergreifende Kommunikation geleitet. Er gehört der Geschäftsleitung der ComConsult Beratung und Planung GmbH an und betätigt sich als Berater, Autor und Seminarleiter.

Herr Meder ist im Team der ComConsult Beratung und Planung GmbH als Senior Consultant beschäftigt. Er verfügt aufgrund seiner langjährigen beruflichen Praxis über umfangreiche Kenntnisse und Erfahrungen aus den Bereichen Konzipierung und Betrieb von Netzwerken. Sein Themenschwerpunkt als Berater und Planer liegt in den Bereichen Internetworking und IT-Security. Zu diesen Themengebieten ist er als Referent bei der ComConsult Akademie tätig.

Fax-Antwort an ComConsult 02408/955-399

# Bestellung
# Wide Area Networks:
## Technik und Funktionsweise

Ich bestelle den Report
☐ **Wide Area Networks: Technik und Funktionsweise**
Preis von € 398,- zzgl. MwSt. und Versand (Mai 2009)

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

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

Neuauflage Technologie-Report

# Wide Area Networks:
## Leitfaden für Design, Ausschreibung und Betrieb

**Soeben ist der Report „Wide Area Networks: Leitfaden für Design, Ausschreibung und Betrieb“ von Dr. Behrooz Moayeri und Dipl.-Inform. Andreas Meder erschienen.**

Der neue Report von ComConsult Research befasst sich mit allen Phasen eines WAN-Projektes, nämlich mit den Aspekten „Plan, Build, Run“. Wide Area Networks unterliegen eigenen Gesetzmäßigkeiten, die sie von lokalen Netzen unterscheiden:

- Im WAN sind die Bandbreiten wesentlich niedriger als im LAN, und die Signallaufzeiten sind wesentlich länger. Applikationen, die im LAN gut funktionieren, scheitern möglicherweise im WAN aufgrund der begrenzten WAN-Kapazität oder der langen Delays. Es gilt, Anwendungen an WAN-Bedingungen anzupassen, wenn sie nicht WAN-optimiert sind.
- Die Kapazität im WAN ist teuer und verursacht anders als im LAN hohe laufende Kosten. Der Ermittlung des realen Kapazitätsbedarfs kommt daher im WAN-Projekt eine entscheidende Bedeutung zu.
- Die Hochverfügbarkeit im WAN ist bedingt durch lange und komplizierte Übertragungswege schwieriger zu realisieren als im LAN.


- Fast jedes Unternehmen ist im WAN-Bereich auf die Dienste von Service Providern angewiesen. Es gilt, saubere und dem Bedarf des Unternehmens entsprechende Schnittstellen zum Service Provider zu definieren und die Leistungen desselben effizient zu kontrollieren. Dazu dienen die in diesem Report enthaltenen Empfehlungen für WAN-Ausschreibungen.
- Bedingt durch die langen Entfernungen und möglicherweise die internationale Ausprägung des WAN stellt der WAN-Betrieb die Unternehmen vor besondere Herausforderungen.

Der Erfolg eines WAN-Projektes hängt von der Berücksichtigung dieser Besonderheiten ab.

Als Ergänzung zum Report „Wide Area Networks: Technik und Funktionsweise“ fasst das vorliegende Dokument die aktuellen Trends und Erfahrungen aus den letzten WAN-Projekten der ComConsult Beratung und Planung GmbH zusammen.

Die Autoren dieses Reports sind Dr.-Ing. Behrooz Moayeri und Dipl.-Inform. Andreas Meder. Herr Moayeri hat viele Großprojekte mit dem Schwerpunkt standortübergreifende Kommunikation geleitet. Er gehört der Geschäftsleitung der ComConsult Beratung und Planung GmbH an und betätigt sich als Berater, Autor und Seminarleiter.

Herr Meder ist im Team der ComConsult Beratung und Planung GmbH als Senior Consultant beschäftigt. Er verfügt aufgrund seiner langjährigen beruflichen Praxis über umfangreiche Kenntnisse und Erfahrungen aus den Bereichen Konzipierung und Betrieb von Netzwerken. Sein Themenschwerpunkt als Berater und Planer liegt in den Bereichen Internetworking und IT-Security. Zu diesen Themengebieten ist er als Referent bei der ComConsult Akademie tätig.

Beide Reports zum Thema „Wide Area Networks“ sind als WAN-Collection zum Sonderpreis bestellbar.

Fax-Antwort an ComConsult 02408/955-399

# Bestellung
# Wide Area Networks:
## Leitfaden für Design, Ausschreibung und Betrieb

Ich bestelle den Report
☐ **Wide Area Networks: Leitfaden für Design, Ausschreibung und Betrieb**
Preis von € 398,- zzgl. MwSt. und Versand (Mai 2009)

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

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

Schwerpunktthema

Dipl.-Inform. Matthias Egerland ist Leiter des Competence Centers Virtuelle IT und arbeitet als Berater in den Competence Centern IT-Sicherheit und Netze bei der ComConsult Beratung und Planung GmbH. Neben den Schwerpunkten Desktop-, Server- und Infrastruktur-Virtualisierung beschäftigt sich Herr Egerland insbesondere mit der Sicherheit in virtualisierten Umgebungen. Darüber hinaus erstellt er Konzepte und Ausschreibungen von IT-Infrastruktur-Lösungen gemäß UfAB. Herr Egerland ist zertifiziert als Cisco Certified Network Associate (CCNA).

Dipl.-Ing. Björn Korall ist Berater und Netzwerkplaner der ComConsult Beratung und Planung. Bereits während seines Studiums beschäftigte er sich mit drahtloser Datenkommunikation und war in de vergangenen zwei Jahren ausschließlich im Bereich Forschung, Entwicklung und Beratung von WLANs nach IEEE 802.11 tätig. Sein Fokus lag hierbei in der in der Erhöhung der Performance von WLANs und VoIP over WLAN (VoWLAN).

Dipl.-Inform. Daniel Meinhold ist Consultant bei der ComConsult Beratung und Planung GmbH. Dort ist er in den Bereichen Telekommunikationsysteme, Virtualisierung und IT-Sicherheit tätig. Neben diesbezüglichen Praxiserfahrungen in zahlreichen Projekten ist er für die Planung und Durchführung entsprechender Testszenarien im ComConsult-eigenen Labor zuständig.

# Virtualisierung: Mehr Sicherheit durch virtuelle Firewalls?

Fortsetzung von Seite 1

### 1. Sicherheitsstrukturen mit unterschiedlichem Virtualisierungsgrad

Der Einsatz von Server-Virtualisierung hat sich mittlerweile in vielen Unternehmen und Behörden etabliert. Die Absicherung virtueller Serverumgebungen erfordert hierbei die Berücksichtigung von unterschiedlichen Vertrauensbereichen, z.B. Finanz-, Produktions- und Testumgebung. Die Gruppierung der virtuellen Server eines Vertrauensbereiches zu einer Sicherheitszone ist hierbei je nach Anforderung an Sicherheit, Verfügbarkeit und Performance auf unterschiedliche Art möglich. Grundsätzlich kann zwischen drei Architekturen unterschieden werden, welche nachfolgend kurz erläutert werden. Detaillierte Informationen zu Sicherheitszonen in virtuellen und physischen Umgebungen finden sich im Netzwerk Insider vom November 2008 :

#### 1.1 Szenario 1: Dedizierte physische Server je Sicherheitszone

In diesem Szenario werden physische Server dediziert einer Sicherheitszone zugewiesen, z.B. ein Virtualisierungs-Cluster für die Finanzabteilung, ein Virtualisierungs-Cluster für die Entwicklungsabteilung, etc. Physische Sicherheitselemente trennen, wie zuvor ohne Virtualisierung, die verschiedenen Sicherheitszonen voneinander ab (siehe Abbildung 1).

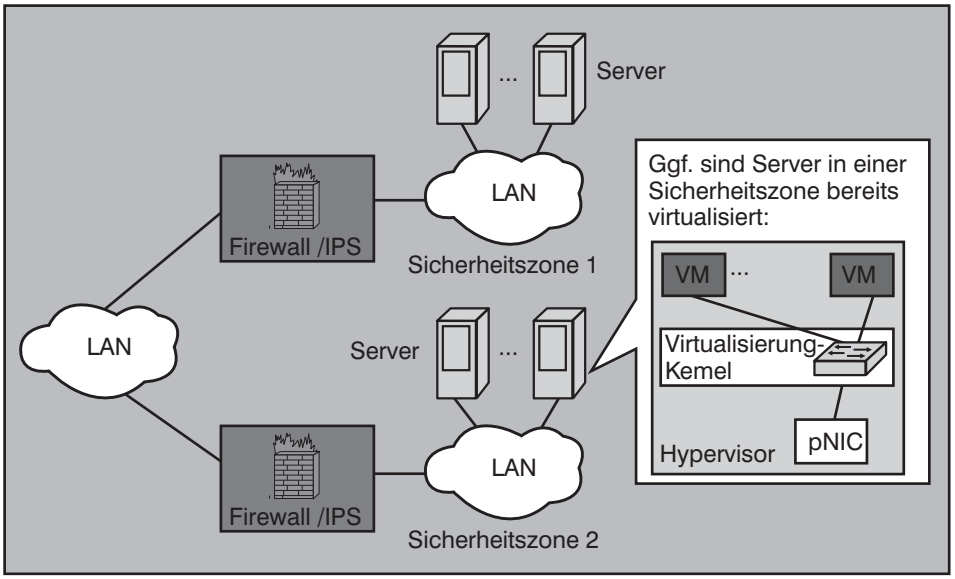



Abbildung 1: Dedizierte physische Server je Sicherheitszone

### 1.2 Szenario 2: Virtuelle Trennung von Sicherheitszonen

Im zweiten Szenario erfolgt die Trennung innerhalb der virtuellen Umgebung mittels virtueller Switche. Diese werden dediziert oder mittels VLAN-Tagging einer physischen Netzwerkschnittstelle (pNIC) zugeordnet und an externe physische Sicherheitselemente angebunden (Abbildung 2).

heiten abhängig, wie z.B. NICs, Switches, Routern oder anderen Sicherheitselementen. Eine virtualisierte Umgebung erfordert, dass dieser Netz- bzw. Sicherheitskontext (aktuelle Zustände/ Sitzungen, VLANs, QoS-Parameter, Traffic-Zähler etc.) dynamisch auf allen Host-Systemen zur Verfügung steht. Diese Kontexte müssen insbesondere bei dynamischen Leistungsmerkmalen der Virtualisierungslösung nicht nur erhalten, sondern auch konsistent bleiben. Als Beispiele solcher Leistungsmerkmale seien an dieser Stelle VMware HA, VMotion, Citrix XenMotion bzw. Microsoft Live Migration sowie dynamische Ressourcenverteilung durch z.B. VMwares Distributed Ressource Scheduler (DRS) genannt.

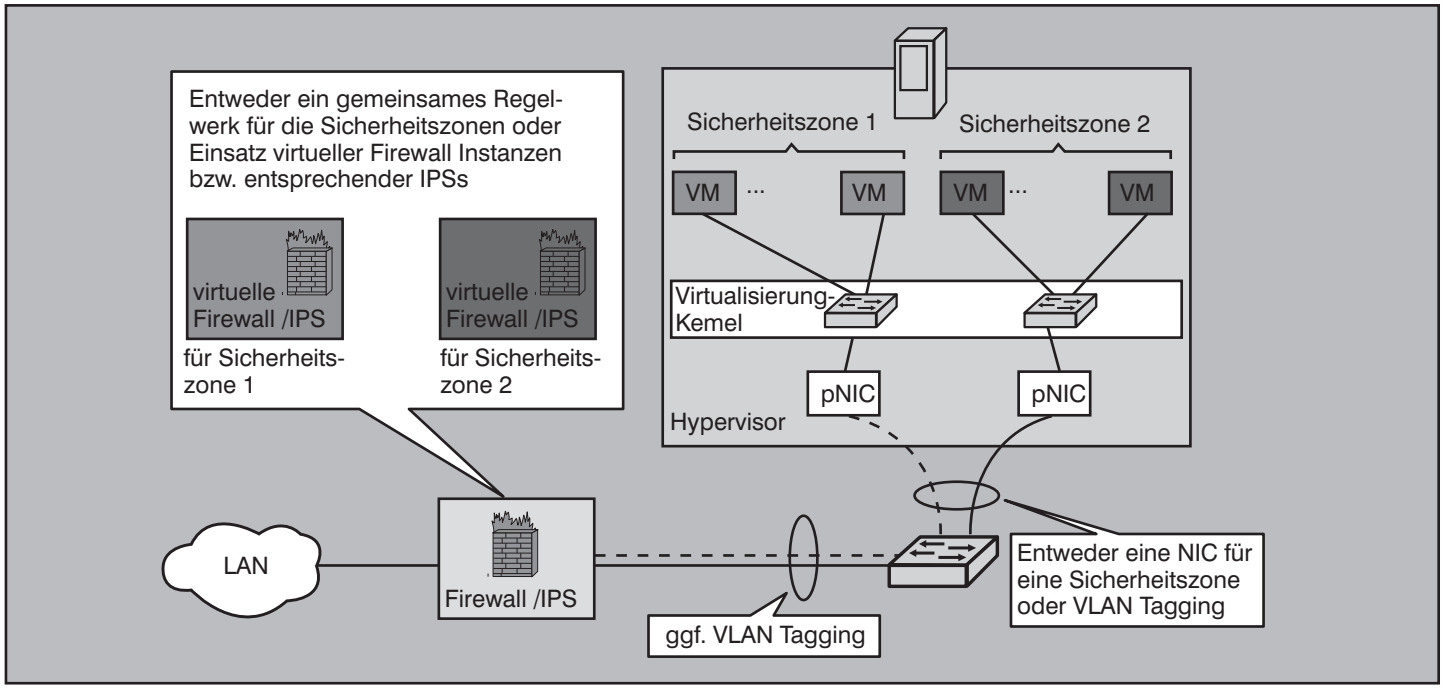



Abbildung 2: Virtuelle Trennung von Sicherheitszonen

### 1.3 Szenario 3: Vollständige Virtualisierung

Ähnlich wie in Szenario 2 werden auch hier die Sicherheitszonen innerhalb der virtuellen Umgebungen gebildet. Anstatt diese jedoch über physische Sicherheitselemente zu führen, kommen diese in virtualisierter Form zur Anwendung, z.B. virtuelle Firewalls oder IDS/IPS-Systeme (Abbildung 3).

Als Richtlinie gilt in dieser Architektur, dass das Sicherheitsniveau je nach Virtualisierungsgrad abnimmt, d.h. das höchste Sicherheitsniveau wird mittels dedizierter physischer Server für die virtuellen Server eines Vertrauensbereiches erzielt (Szenario 1). Dies steht im Widerspruch zu den grundsätzlichen Vorteilen, die durch die Virtualisierung erreicht werden sollen, wie z.B. einer effizienteren Auslastung der Systeme.

Doch auch die Verwendung von virtuellen Sicherheitselementen, wie in den Szenarien 2 und 3 dargestellt, stellt eine Herausforderung dar. In physischen Infrastrukturen sind Sicherheitsarchitekturen hochgradig von physischen Gegeben-

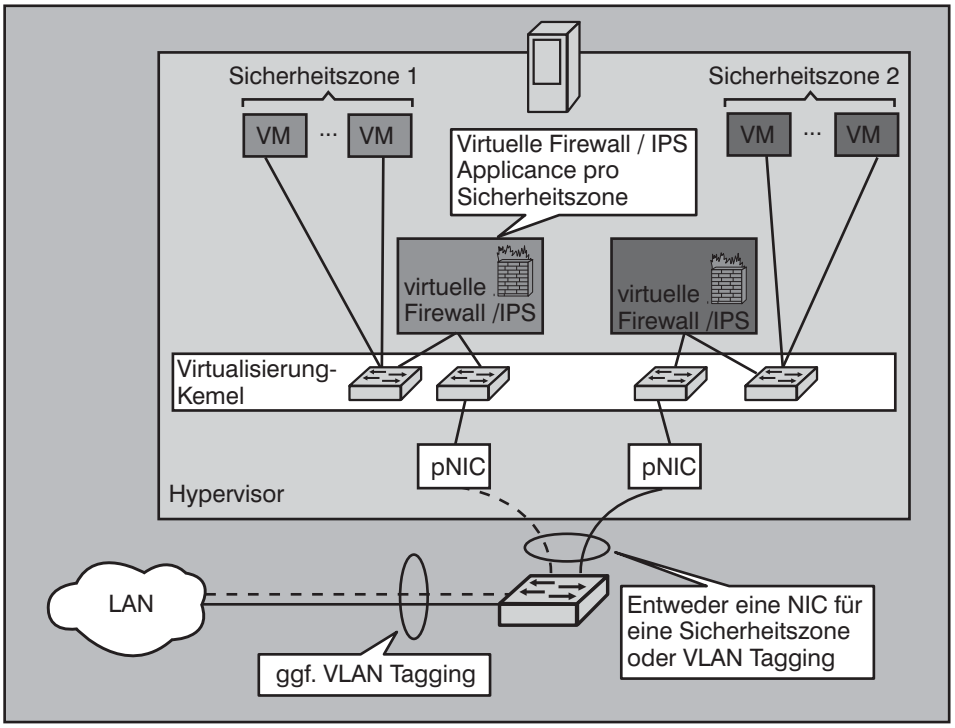



Abbildung 3: Vollständige Virtualisierung von Sicherheitszonen

Ein weiterer wichtiger Aspekt im Zusammenhang mit virtuellen Firewalls ist die erforderliche Performance für den Betrieb der virtuellen Sicherheitskomponenten, welche nun logischerweise mit in die Ressourcenplanung bzw. die Dimensionierung der virtuellen Infrastruktur integriert werden müssen. In physischen Firewalls kommt oftmals Spezialhardware zum Einsatz, welche auf die Anforderungen der Paketanalyse optimiert ist. Beispielsweise werden speziell entworfene ASICs zur Paket- und Flussanalyse verwendet. Eine derart optimierte Hardware ist nicht ohne Leistungsverlust zu virtualisieren.

### 2. Begriffsklärung

Da es – wie im letzten Abschnitt dargestellt – zwei grundlegend unterschiedliche Ansätze gibt, Firewalls zu virtualisieren, ist zunächst eine Begriffsklärung erforderlich, wenn von „virtuellen Firewalls“ die Rede ist. Die folgenden Abschnitte grenzen „virtualisierbare“ von den „virtuellen“ Firewalls ab und zeigen die konzeptionellen Unterschiede beider Varianten auf.

#### 2.1 Virtualisierbare Firewalls – Appliances, die in logische Firewall-Instanzen untergliedert werden können

Die meisten am Markt etablierten Hersteller von Appliance-basierten Firewalls- also Firewalls, die als physische Komponente in das Datennetz integriert werden - bieten bereits seit geraumer Zeit das Leistungsmerkmal, ihre Komponenten in logische Firewall-Instanzen zu segmentieren. Jede Teileinheit stellt sich nach Außen als eigene Firewall dar, die unabhängig von benachbarten Teileinheiten ein eigenes Regelwerk, eigene Administrationsrechte, eigene IP-Adressstrukturen und ggf. eigene Routing-Tabellen besitzt.

Innerhalb von mandantenfähigen Firewall-Managementsystemen können diese Firewall-Instanzen wie ihre physischen Pendants überwacht und administriert werden. Dem Firewall-Manager einer einzelnen Instanz können granular Rechte vergeben werden, die es ihm in einem bestimmten Umfang erlauben, seine Instanz zu verwalten. Ein übergeordnetes Basisregelwerk, Netzwerkeinstellungen sowie bestimmte Objekte können beim Anlegen der Instanz vordefiniert und gleichzeitig für die jeweilige Instanz vor Änderung geschützt werden. Damit bieten virtualisierbare Firewalls die Möglichkeit, Mandanten einfach und kostengünstig eine vollwertige Firewall zur Verfügung zu stellen, ohne auf eine übergeordnete Basiskontrolle verzichten zu müssen.

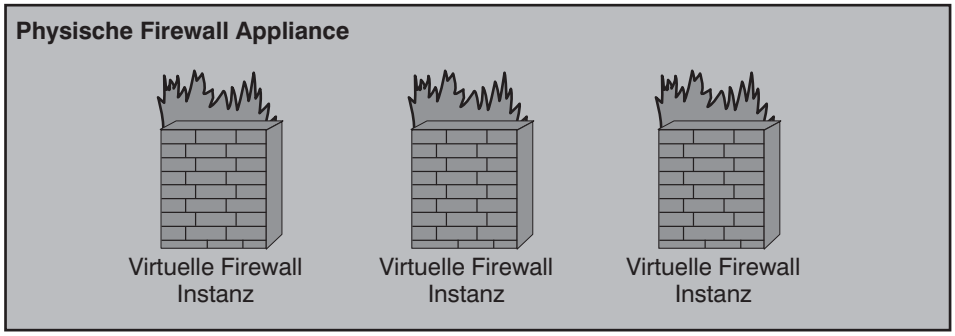



Abbildung 4: Physische Firewall mit drei virtuellen Firewall Instanzen

Eine solche physische Sicherheitskomponente soll im Folgenden als „virtualisierbare Firewall“ bezeichnet werden, während die darin konfigurierten einzelnen logischen Firewalls „virtuelle Firewall Instanzen“ darstellen.

Die einzelnen am Markt befindlichen Produkte dieser Kategorie unterscheiden sich hinsichtlich der Frage, welche der genannten Leistungsmerkmale zu welchem Grad unabhängig von benachbarten virtuellen Firewall Instanzen verfügbar sind. Beispiele für diese Architektur sind Ciscos „Virtual Firewall Context“, Junipers „Virtual System“ und Nokias „Multiple Domain Security“.

Abbildung 4 zeigt eine physische Firewall Appliance, in der drei logische Firewalls in Form von virtuellen Firewall Instanzen konfiguriert sind.

#### 2.2 Virtuelle Firewalls – Firewalls als virtuelle Maschine innerhalb einer Server-Virtualisierungslösung

Mit der Marktreife von Technologien zur Server-Virtualisierung hält nun auch eine weitere Form von Firewalls Einzug in das Portfolio der Anbieter von Sicherheitskomponenten: Firewalls, die als virtuelle Maschine innerhalb einer Virtualisierungsumgebung betrieben werden. Mit derartigen Produkten sind insbesondere diejenigen Hersteller am Markt zu finden, deren Firewalls auch ohne den Virtualisierungsgedanken als reine Software-Lösung erhältlich sind bzw. für Standard-(Linux-)-Betriebssystem-Umgebungen entwickelt wurden. Als Beispiele derartiger Anbieter sind Checkpoint mit der VPN-1 VE „Virtual Edition“ und Astaro mit der „Security Gateway Virtual Appliance“ zu nennen.

Der Leistungsumfang dieser Komponenten geht dabei über den eines dynamischen Paketfilters deutlich hinaus: VPN-Gateway, Intrusion Prevention, E-Mail-Sicherheit bis hin zu Hochverfügbarkeit im Active/Active- und Active/Standby-Modus gehören zum Funktionsumfang der genannten Produkte. Dabei werden jedoch seitens der Hersteller keine Angaben zur Leistung in diesen Kategorien gemacht. Dies ist insofern verständlich, als die Leistung von den verfügbaren Ressourcen des Host-Systems abhängt. Hier sollte ein ausgiebiger Test mit realistischen Kommunikationsdaten in einem nicht-produktiven Umfeld der weiteren Einsatzplanung vorausgehen. Schließlich wird eine solche Sicherheitskomponente schnell zum Flaschenhals, wenn sie sämtlichen Netzverkehr auf mehreren Schichten des OSI-Modells untersuchen soll. Und nicht umsonst wurde auf Seiten der physischen Sicherheits-Appliances Spezialhardware entwickelt, die nur auf Basis von dedizierten ASICs hohe Durchsatzraten erzielen kann.

Die Produktion einer virtuellen Appliance ist bei Vorliegen einer reinen Software-Lösung aus Herstellersicht denkbar einfach: Innerhalb einer Virtualisierungsumgebung wie beispielsweise Citrix XenServer, Microsoft Hyper-V oder VMware Virtual Infrastructure wird eine neue virtuelle Maschine angelegt, die das erforderliche Betriebssystem aufweist und über die nötigen I/O-Ressourcen zur Kommunikation der VM mit der Außenwelt verfügt. Diese virtuelle Maschine erhält Zugriff auf die Firewall-Software z.B. in Form eines ISO-Images der Installations-CD-ROM, die mit einem virtuellen CD-ROM-Laufwerk verknüpft ist. Die Software wird nun von diesem Image auf die virtuelle Maschine installiert. Nachdem der Installationsvorgang abgeschlossen ist, liegt die virtuelle Appliance in Form des Festplatten-Images der virtuellen Maschine vor.

Ist dieses Festplatten-Image in einem offenen Format spezifiziert, wie etwa Microsofts „Virtual Harddisk“ (.vhd) oder dem „Open Virtual File Format“ (.ovf), ist diese virtuelle Maschine theoretisch mit jeder Server-Virtualisierungslösung zu betreiben, die dieses Format unterstützt. In der Praxis ist es gegenwärtig so, dass die meisten Hersteller derartiger virtueller

Firewalls das VMware-proprietäre „Virtual Machine Disk Format“ (.vmdk) nutzen. Der Hintergrund dafür ist, dass VMware ein eigenes Zertifizierungsprogramm aufgelegt hat, das ein Produkt als „VMware Certified Virtual Appliance“ ausweist, sofern es im Wesentlich die folgenden Aspekte liefert:

- fertige Konfektion der Software als virtuelle Maschine für die Virtualisierungslösung von VMware
- Support des Herstellers für den Betrieb der Software als virtuelle Maschine in der VMware-Umgebung
- Lizenzgebühren des Herstellers an VMware

Mindestanforderungen hinsichtlich Funktionalität, Funktionstests oder Leistungsfähigkeit bestehen hingegen nicht.

Theoretisch ist also der Betrieb der virtuellen Appliance auch im Citrix XenServer und Microsoft Hyper-V Umfeld denkbar, nachdem das Dateiformat in die dort lesbare „.vhd“-Form konvertiert wurde. Allerdings würde dann der Hersteller-Support für diese Lösung nicht mehr gelten, weswegen diese Möglichkeit in Produktivumgebungen ausscheidet.

Das Management dieser virtuellen Firewalls unterscheidet sich nicht von ihren physischen Ausführungen. Beide werden über das gleiche zentrale Management verwaltet. Die Virtualisierung bleibt somit hinsichtlich des Managements transparent für den Firewallbetrieb.

Die folgenden Abschnitte beleuchten Integrationsaspekte sowie Hochverfügbarkeitsmechanismen derartiger virtueller Firewalls.

### 3. Integration in die virtuelle Infrastruktur / das Datennetz

Die marktgängigen Server-Virtualisierungslösungen vom Typ 1 Virtual Maschine Monitor arbeiten nach dem Prinzip, dass auf einer geeigneten Serverhardware eine Virtualisierungslösung installiert wird – der sog. Hypervisor – auf dem dann die virtualisierten Server in Form von virtuellen Maschinen (VMs) laufen. Um den virtuellen Maschinen eine Netzwerkverbindung sowohl untereinander, als auch mit der Außenwelt zu ermöglichen, werden virtuelle Netzwerke (Citrix) bzw. virtuelle Switches (VMware) innerhalb des Hypervisors realisiert.

Während sich die Bezeichnung dieses Ansatzes zwischen den Herstellern der Virtualisierungslösungen unterscheidet, ist die damit verbundene Funktionalität die gleiche: mit Hilfe der Administrationsoberfläche oder Kommandozeile wird für jede physische und virtuelle Netzwerkschnittstelle definiert, welchem Netzwerk diese zugeordnet wird, welche VLAN ID sie ggf. bekommt und welche Konnektivität sich daraus mit anderen Netzwerkschnittstellen ergibt. Auf diese Weise können unterschiedliche Topologien realisiert werden: Testumgebungen ohne Verbindung zur Außenwelt oder dem Produktivnetz, Demilitarisierte Zonen (DMZ) innerhalb der Virtualisierungsumgebung und Servernetze mit Verbindung zum physischen LAN.

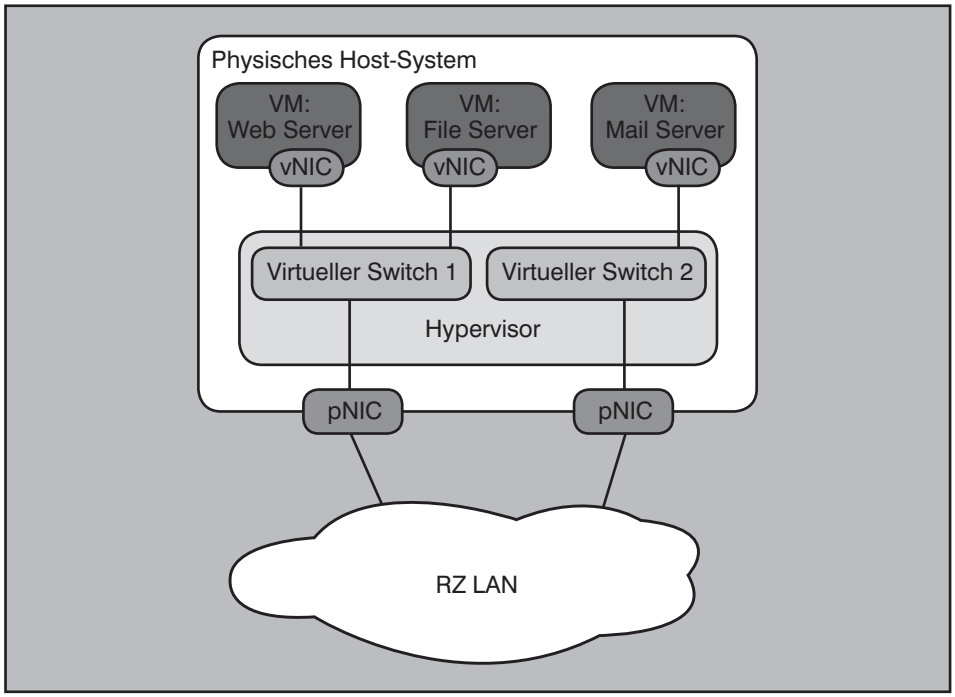



Abbildung 5: Verbindung der virtuellen Maschinen untereinander und mit dem physischen Netz (RZ LAN) über virtuelle Switches innerhalb des Hypervisors. Physische Netzwerkschnittstellen (pNIC) verbinden das Host-System mit dem Rechenzentrumsnetz, virtuelle Netzwerkschnittstellen (vNIC) verbinden die virtuellen Maschinen mit den virtuellen Switches.

Abbildung 5 zeigt die Verbindung von virtuellen Maschinen untereinander und mit dem physischen Netz (RZ LAN) über virtuelle Switches innerhalb des Hypervisors.

Die von VMware gewählte Bezeichnung „virtueller Switch“ mag dabei zur Veranschaulichung der Funktionalität dieser Komponente dienlich sein. Andererseits ist sie insofern irreführend, als dem virtuellen Switch einige wesentliche Merkmale fehlen, die der Netzwerker mit einer solchen Komponente assoziiert. So besitzt der virtuelle Switch zwar ebenfalls eine MAC-Tabelle, in der er die Zuordnung von Layer-2-Adressen und seinen einzelnen Ports speichert. Diese MAC-Tabelle wird jedoch nicht dynamisch auf Basis des beobachteten Datenverkehrs erlernt, sondern mittels der oben beschriebenen statisch konfigurierten Konnektivität definiert. Ein Ethernet-Frame mit einer unbekannten Ziel-MAC-Adresse führt also nicht zu einem Layer-2-Broadcast an alle Switch-Ports, sondern wird schlicht verworfen.

Aus einer Sicherheitsperspektive betrachtet bringt dieses Verhalten des virtuellen Switches jedoch auch Vorteile mit sich: konstruktionsbedingt ist diese Komponente unempfindlich gegenüber Layer-2-Angriffen wie beispielsweise MAC-Flooding. Beim MAC-Flooding wird durch eine große Zahl von Ethernet-Frames mit unterschiedlicher Source-MAC-Adresse versucht, die MAC-Tabelle des Switches zum Überlaufen zu bringen und ihn dadurch zu kompromittieren. Da der virtuelle Switch neue MAC-Adressen nicht dynamisch lernt, kann seine MAC-Tabelle auch nicht überlaufen.

Ein weiterer wesentlicher Unterschied zu physischen Switches ist, dass virtuelle Switches innerhalb eines Hypervisors nicht untereinander verbunden werden können. Es können also keine hierarchischen oder redundanten Netztopologien innerhalb des Hypervisors aufgebaut werden, wie sie aus physischen Netzumgebungen bekannt sind. Dieser Umstand bringt den Vorteil mit sich, dass mittels virtueller Switche keine Schleifentopologien konfiguriert

werden können. Damit müssen Mechanismen zur Schleifenunterdrückung wie beispielsweise das Spanning Tree Protocol (STP) von diesen Komponenten nicht unterstützt werden. Auch zwischen zwei physischen Netzwerkschnittstellen, die mit dem gleichen virtuellen Switch verbunden sind und im „NIC-Teaming"-Modus betrieben werden, erfolgt kein Switching.

Ein weiterer Vorteil der Tatsache, dass die Bezeichnung „virtuelles Netzwerk" von Citrix in Anbetracht der realisierten Funktionalität treffender ist als „virtueller Switch" von VMware, ist der damit ausbleibende Einfluss auf die physische Netztopologie. Durch die virtuellen Switches wird eben keine weitere Ebene in die Netzwerkhierarchie eingezogen. Bei Inbetriebnahme einer der heutigen Server-Virtualisierungslösungen muss das Netzdesign nicht angepasst werden. Spanning-Tree-Domänen dehnen sich genauso wenig in die virtuelle Infrastruktur aus wie Routing-Bereiche.

Dies mag sich in dem Moment ändern, wo ein tatsächlich vollwertiger virtueller Switch in die Virtualisierungsumgebung eingebracht wird, wie beispielsweise der Cisco Nexus 1000v. Hier gilt es genau zu analysieren, ob ein physischer Switch mit allen Leistungsmerkmalen aber auch Einflüssen auf die Netztopologie virtualisiert wurde, oder ob das oben beschriebene Konzept der virtuellen Switches um zusätzliche Funktionalitäten wie erweiterte Port Security und Quality of Service ergänzt werden.

Virtuelle Firewall-Appliances sind aus Sicht des Host-Systems eine virtuelle Maschine wie jede andere auch und werden insofern in gleicher Weise mit dem Netzwerk verbunden. Abbildung 6 zeigt die Realisierung einer DMZ mittels virtueller Switches und einer virtuellen Firewall in einer virtuellen Umgebung.

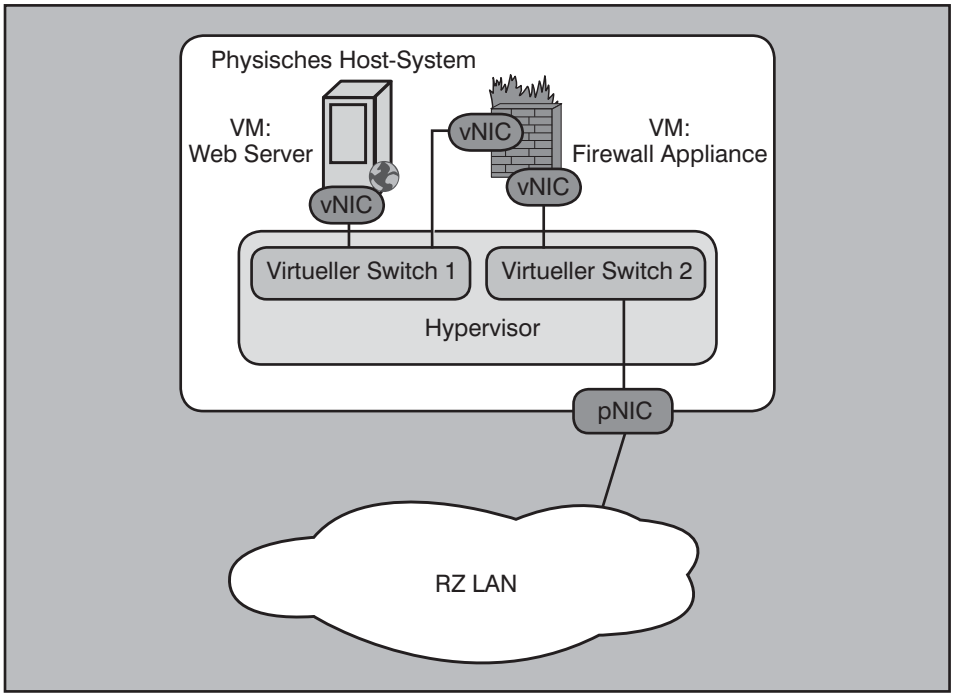



Abbildung 6: Realisierung einer DMZ mittels virtueller Switches und einer virtuellen Firewall in einer virtuellen Umgebung

### 4. Hochverfügbarkeit von virtuellen Firewalls

Die Anforderungen an die Verfügbarkeit von Netzkomponenten und Servern sind in virtuellen Umgebungen nicht anders als in physischen Netzen. Dies gilt insbesondere auch für Sicherheitskomponenten, von deren Verfügbarkeit in der Regel die Erreichbarkeit ganzer Netzbereiche abhängt.

Beim Einsatz physischer Appliances in herkömmlichen, nicht-virtualisierten Server-Umgebungen wird üblicherweise ein Active/Standby-Betrieb der Appliances favorisiert, da hier eine vollwertige Redundanz und ein deterministischer Kommunikationspfad vorliegt. Bei Interface-Problemen oder Ausfall der aktiven Firewall übernimmt die Standby-Firewall und wechselt in den aktiven Status. Die Auswirkungen auf die Verkehrsflüsse innerhalb der Schutzzone sind marginal. Da im Layer-3-Modus betriebene Firewall-Cluster über virtuelle IPs verfügen, welche dynamisch der aktiven Firewall zugeordnet werden, muss es bei einem Schwenk lediglich zu einem Update der MAC-Tabellen auf den mit dem Cluster verbundenen Layer-2-Komponenten kommen. Damit besteht der Unterschied bei einem Schwenk im Wesentlichen aus einem neuen Pfad, den die Pakete durch das Netzwerk nehmen. Aus logischer Sicht hingegen ändert sich nichts.

Ein solcher Hochverfügbarkeitsmechanismus muss auch von virtuellen Firewalls unterstützt werden. Auch virtuelle Firewalls müssen entweder im Active/Active- oder im Active/Standby-Modus redundant

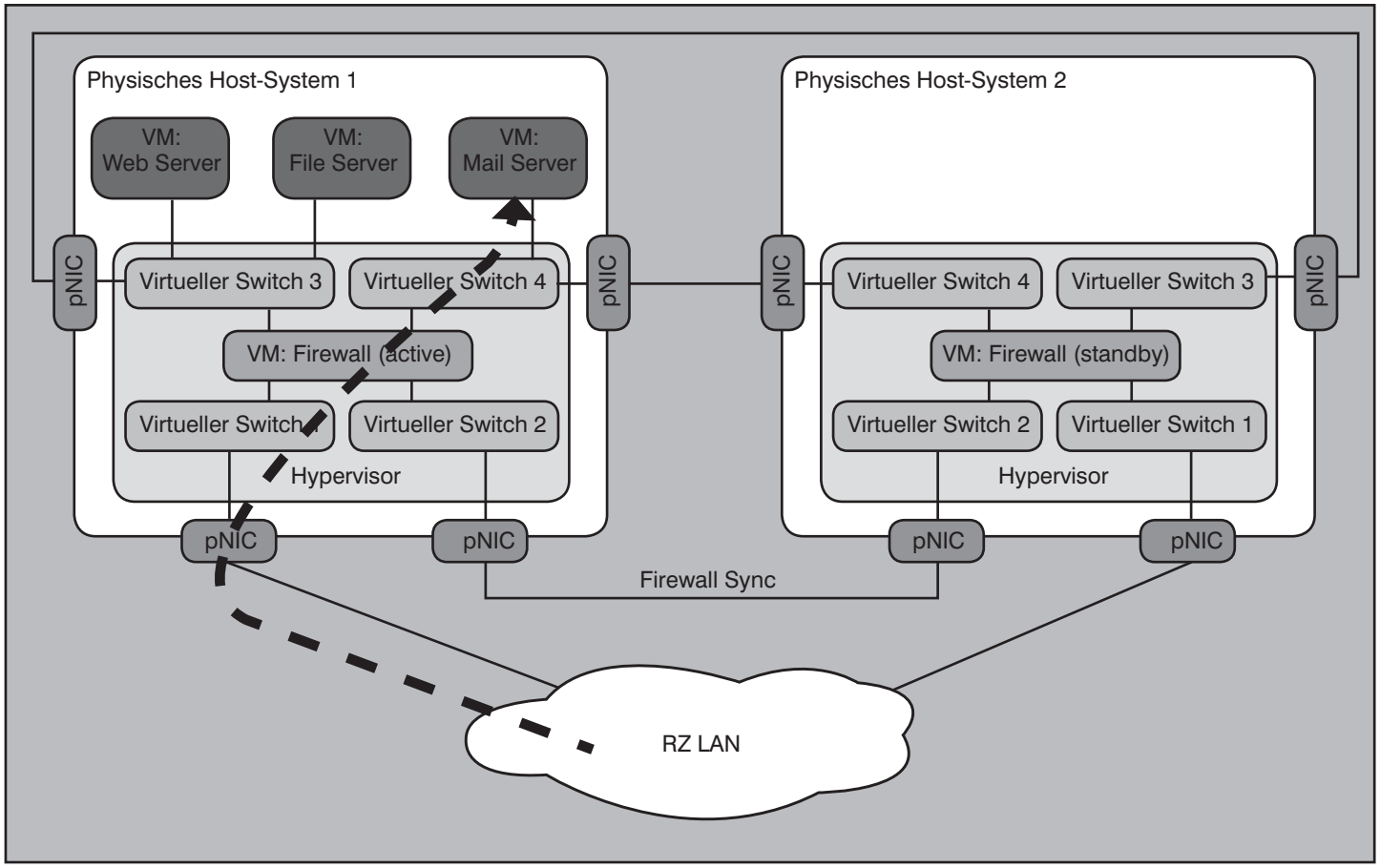



Abbildung 7: Aufbau eines redundanten Host-Systems mit redundanten virtuellen Firewalls und drei virtuellen Servern. Die virtuellen Switches 3 und 4 bilden virtuelle „Server Switches“. Die gestrichelte Linie zeigt den Kommunikationspfad zum Mail Server im Normalbetrieb.

ausgeführt und auf unterschiedlichen physischen Host-Systemen zum Einsatz gebracht werden können.

Bei der Integration einer redundant ausgeführten virtuellen Firewall in die virtuelle Netzumgebung der Virtualisierungslösung ergeben sich jedoch einige Besonderheiten, die bei der Planung des physischen Netzes und der Dimensionierung der Host-Systeme zu berücksichtigen sind.

Wie in einer physischen Umgebung auch, müssen die redundanten Firewalls Statusinformationen synchronisieren und Heartbeat-Signale austauschen. Hierfür sind eine dedizierte Netzverbindung und jeweils ein virtueller Switch erforderlich. Die Außenanbindung über die physische Netzwerkschnittstelle, die mit dem Rechenzentrumsnetz verbunden ist, wird ebenfalls über einen eigenen virtuellen Switch realisiert. Die virtuellen Server werden über eigene virtuelle Switches angebunden, die sich logisch hinter der Firewall befinden. Abbildung 7 zeigt diesen Aufbau, bei dem drei virtuelle Maschinen (Web Server, File Server und Mail Server) in zwei unterschiedlichen Servernetzen (virtueller Switch 3 und 4) durch eine virtuelle Firewall geschützt werden.

### 4.1 Verschiebung einzelner virtueller Maschinen

Der zweite physische Host, auf dem die redundante virtuelle Firewall installiert ist, muss mit den gleichen Netzen konfiguriert sein wie der erste Host, damit er im Fehlerfall dessen Aufgaben übernehmen kann. Genau hier liegt eines der Interferenzpotentiale mit den Eigenschaften der Virtualisierungslösung: Im Fall von VMware Virtual Infrastructure führt der HA-Cluster-Betrieb der ESX-Hosts im Fehlerfall dazu, dass sämtliche virtuelle Maschinen auf dem verbleibenden Host neu gestartet werden. Demnach würde auch die aktive virtuelle Firewall auf dem zweiten Host gestartet, obwohl dort zwischenzeitlich die redundante Firewall ihre Aufgabe übernommen hat. Dies führt nicht zwangsläufig zu einem Konflikt, wenn die neu gestartete Firewall aufgrund des Heartbeats der redundanten Firewall im Standby-Modus läuft. Dennoch ist diese HA-Eigenschaft in der Regel nicht erwünscht.

Um dieses Verhalten auf einem Zwei-Knoten-Cluster zu vermeiden, sind Priorisierungsmöglichkeiten erforderlich, wie sie etwa die Citrix XenServer Virtualisierungslösung bietet, mit der die HA-Eigenschaft je virtueller Maschine definiert und bis auf 0 reduziert werden kann. Auch unter Microsoft Hyper-V käme es nicht zu diesem Konflikt, da einzelne virtuelle Maschinen – und so auch die virtuelle Firewall – entweder als geclusterter oder nicht-redundanter Dienst eingerichtet werden können.

Ebenso müssen für virtuelle Firewalls dynamische Mechanismen zur Lastverteilung deaktiviert werden, wie z.B. VMwares Distributed Ressource Scheduler (DRS). Würde aufgrund einer vorliegenden Lastsituation die virtuelle Firewall im laufenden Betrieb auf ein anderes Host-System migriert, erhielte das Rechenzentrumsnetz keine Kenntnis von der damit einhergehenden Veränderung in der netzwerkseitigen Erreichbarkeit der von der Firewall geschützten virtuellen Maschinen. Neben der zwar kurzen aber dennoch registrierbaren Downtime, die die Migration der virtuellen Firewall mit sich bringt, müssen die MAC-Tabellen der physischen RZ-Switches der neuen Situation angepasst werden. Wird

dies nicht durch proaktives Verhalten der verschobenen Firewall (z.B. in Form von Gratuitous ARPs) unterstützt, kommt es zu längeren Ausfällen.

Auf Cluster-Systemen mit mehr als zwei Knoten kann diesem Problem durch Konfiguration einer negativen Affinität für beide virtuelle Firewalls begegnet werden. Im Fall eines erforderlichen Umzugs bzw. Neustarts der ersten, ursprünglich aktiven Firewall sorgt dieser Mechanismus dafür, dass diese Firewall nicht auf dem gleichen Host-System gestartet wird, auf dem die redundante Firewall läuft.

Wie in Abbildung 7 dargestellt, müssen die virtuellen „Server Switches“ 3 und 4 über eine dedizierte Verbindung mit ihrem Pendant auf Seiten des zweiten Host-Systems verbunden werden. Dies hängt damit zusammen, dass neben dem betrachteten Totalausfallszenario eines Host-Systems auch der Umzug einzelner virtueller Maschinen im laufenden Betrieb möglich ist. Dieses in Abhängigkeit der Virtualisierungslösung mit „XenMotion“, „VMotion“ oder „LiveMigration“ bezeichnete Verfahren führt dazu, dass der aktiv genutzte Hauptspeicherbereich einer virtuellen Maschine auf eine Nachbarmaschine umkopiert wird. Ist dieser Vorgang vollständig abgeschlossen, wird der Verweis auf den Festplattenspeicher dieser virtuellen Maschine auf diese neue Instanz umgelenkt und die Maschine läuft auf dem zweiten System weiter, während es von dem ursprünglichen Host-System entfernt werden kann. Dieser Vorgang ist nur möglich, wenn auf dem zweiten Host-System das gleiche virtuelle Netz bzw. der gleiche virtuelle Switch verfügbar ist.

Üblicherweise macht sich eine im laufenden Betrieb verschobene virtuelle Maschine nach Abschluss dieses Vorgangs in Form eines Gratuitous ARPs gegenüber der physischen Infrastruktur bemerkbar. Die physischen Switches passen daraufhin ihre MAC-Tabellen entsprechend an und die virtuelle Maschine ist fortlaufend über den neuen physischen Host erreichbar.

Da im oben beschriebenen Szenario jedoch nur die virtuelle Maschine umgezogen ist, die virtuelle Firewall sich jedoch noch auf dem ursprünglichen Host befindet, ist die Erreichbarkeit des virtuellen Servers immer noch nur durch das erste Host-System möglich. Die virtuelle Firewall auf dem zweiten Host-System läuft weiterhin im Standby-Modus und erlaubt insofern keinen Netzzugriff auf die umgezogene virtuelle Maschine. Wie in Abbildung 8 gezeigt, erfordert dies, dass der Zugriff über die Querverbindung der virtuellen Server Switches 4 beider Host-Systeme erfolgt. Dieser Umstand ist bei der Dimensionierung der physischen Netzwerkschnittstellen zu berücksichtigen. De facto führt er zu der Verdoppelung des Bedarfs an Netzwerkschnittstellen für die Produktivdaten: die gleiche Anzahl und Bandbreite physischer Netzwerkschnittstellen in Richtung Rechenzentrumsnetz (RZ LAN) ist auch noch einmal für diese Querverbindung der virtuellen Server Switches einzuplanen.

Daran ändert auch die logische Segmentierung einer physischen Netzwerkschnittstelle durch Nutzung von VLANs nichts, da dies nur dann ohne Performanceverlust möglich ist, wenn auch in Richtung RZ LAN die gemeinsame Nutzung der Schnittstelle durch VLAN-Bildung nicht als „Durchsatzbremse“ betrachtet wird.

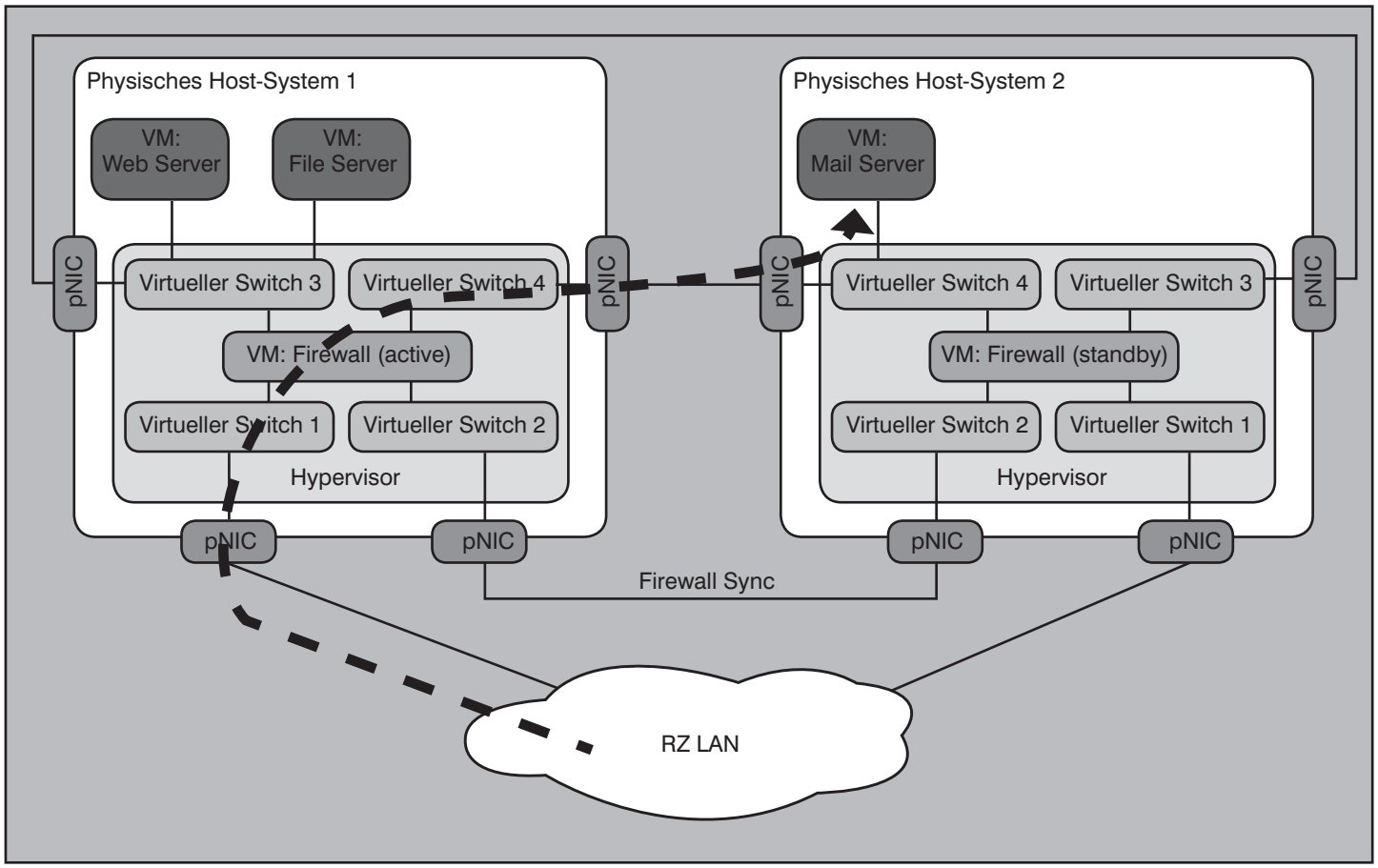



Abbildung 8: Wurde der virtuelle Mail Server im laufenden Betrieb auf den zweiten physischen Host verschoben, bleibt er aufgrund der weiterhin aktiven Firewall über den ersten Host mit dem RZ LAN verbunden. Der Verkehrsfluss wird über eine entsprechende Querverbindung seiner beiden virtuellen Server Switches 4 gelenkt.

Die Anzahl physischer Netzwerkschnittstellen ist jedoch auch ohne diese Betrachtungen bereits ein kritischer Faktor bei der Planung von Server-Virtualisierungsumgebungen. So gilt die Einrichtung folgender dedizierter Netzwerkschnittstellen als „best-practice“:

- 2x Management
- 1x XenMotion / VMotion / LiveMigration
- 1x HA Cluster Heartbeat
- 1x iSCSI (sofern keine Storage-Anbindung per dediziertem HBA)
- 1x Datennetz pro Serverbereich

Da gängige rackmounted Server mit nur bis zu 8 physischen Schnittstellen ausgestattet werden können und man bei Bladesystemen üblicherweise schon mit 6 physischen Schnittstellen an die Midplane die Grenzen der Realisierbarkeit erreicht, gilt es hier im Zuge der Planung einen geeigneten Kompromiss zu finden.

Doch auch bei geeigneter Wahl und Dimensionierung der Schnittstellen führt die wenig intuitive Änderung der Verkehrsflüsse nach einem Fail-Over oder dem Umzug einer virtuellen Maschine dazu, dass das Troubleshooting deutlich erschwert wird. Dies ist auch dann der Fall, wenn – wie im folgenden Abschnitt näher dargestellt – nur die virtuelle Firewall ausfällt und es zu einem Fail-Over auf die redundante virtuelle Firewall kommt.

### 4.2 Failover der virtuellen Firewall

Kommt es zu einer Störung innerhalb der aktiven virtuellen Firewall auf dem ersten physischen Server, erhält die redundante Firewall auf dem zweiten Host-System über die Firewall-Sync-Verbindung hiervon Kenntnis und schaltet in aktiven Betrieb. Hierdurch ändert sich wie in Abbildung 9 dargestellt die Netzwerktopologie. Um eine möglichst unterbrechungsfreie Erreichbarkeit der virtuellen Maschinen zu gewährleisten, muss die virtuelle Firewall das Rechenzentrumsnetz proaktiv über diese geänderte Topologie informieren.

### 4.3 Virtuelle Firewalls im Active/Active-Modus

Zur Philisophie der Server-Virtualisierung gehört eine möglichst gleichmäßige Auslastung aller beteiligten Systeme. Diesem Gedanken widerspricht der Betrieb von zwei Firewalls im Active/Standby-Modus. Dennoch ist auch in virtualisierten Umgebungen ein Active/Active-Betrieb von Sicherheitskomponenten kritisch zu hinterfragen.

Werden die virtuellen Firewalls wie oben beschrieben im Active/Standby-Modus betrieben, ergeben sich die Leistungsanforderungen aus folgenden Aspekten, damit es zu keiner Flaschenhalssituation kommt:

- Die aktive Firewall muss genügend Rechenleistung besitzen, um den Netzverkehr mit der durch die Server-Kommunikation vorgegebenen Datenrate inspizieren zu können.
- Die Netzanbindung der Firewall in Richtung Rechenzentrumsnetz muss so dimensioniert sein, dass die Bandbreite zur Kommunikation mit allen hinter der Firewall liegenden Servern ausreicht.
- Die Querverbindungen zwischen den virtuellen Server Switches müssen ebenfalls so dimensioniert sein, dass die zur Verfügung stehende Bandbreite eine ungehinderte Kommunikation zu allen Servern dieses Netzbereichs

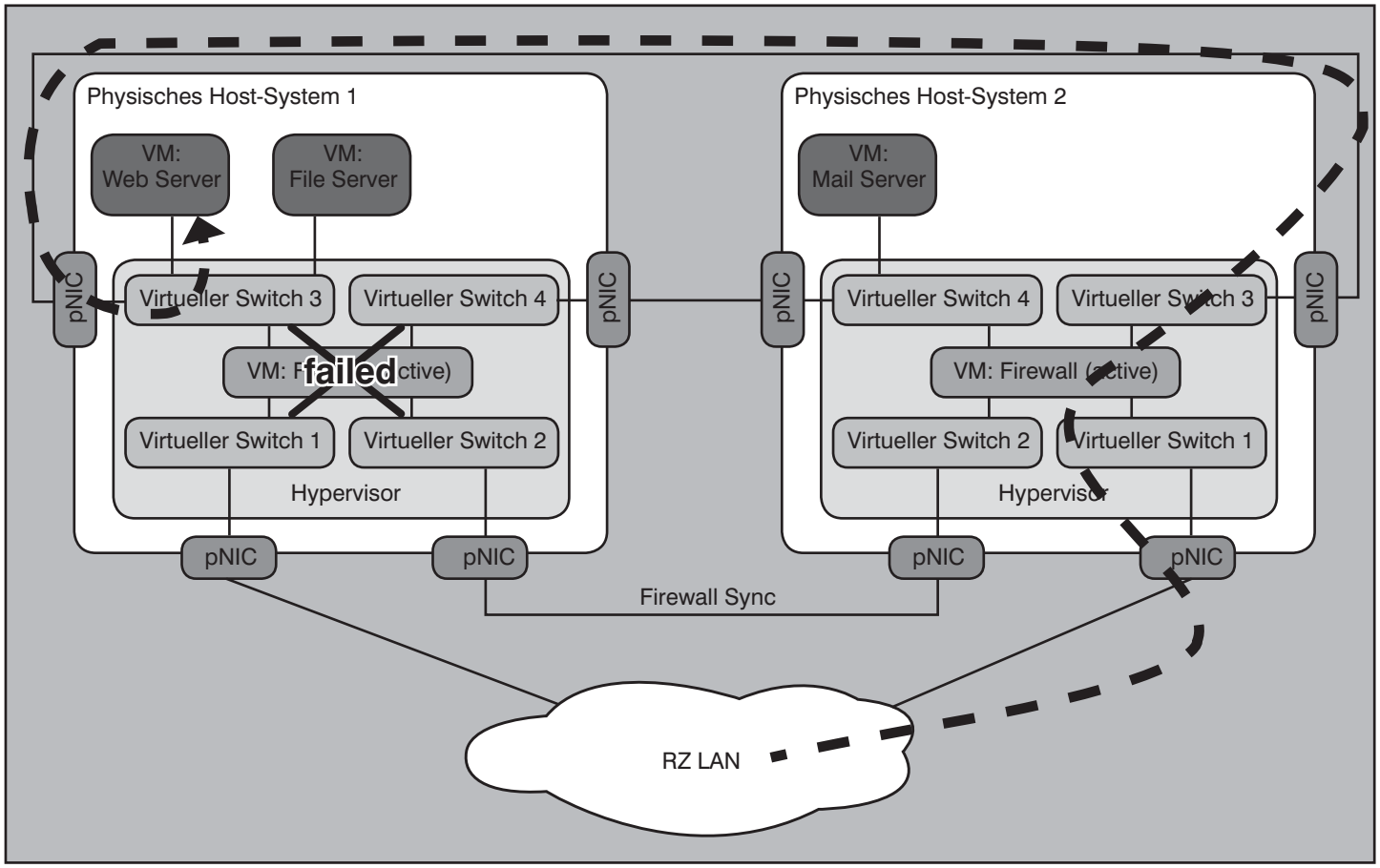



Abbildung 9: Fällt die aktive virtuelle Firewall aus, übernimmt die redundante Firewall auf dem zweiten Host-System und die Verkehrsflüsse in Richtung der virtuellen Server müssen sich entsprechend anpassen.

gestattet, da aufgrund der Dynamik der virtuellen Umgebung die Position einer virtuellen Maschine sich wie oben dargestellt ändern kann.

Der Active/Active-Betrieb von zwei virtuellen Firewalls ergibt für das Gesamtsystem keine Leistungsvorteile:

- Auch wenn im Normalbetrieb jede aktive Firewall nur 50% Last gegenüber dem Active/Standby-Normalbetrieb aufweist, muss das Host-System genügend Ressourcen reservieren, damit im Fehlerfall die verbliebene aktive Firewall die Rolle der ausgefallenen Firewall vollständig übernehmen kann.

- Gleiches gilt für die Dimensionierung der Schnittstellen in Richtung Rechenzentrumsnetz sowie zwischen den virtuellen Server Switches: würde sich aufgrund einer geeigneten Lastverteilung der Netzverkehr zu gleichen Anteilen auf beide Firewalls aufteilen, müssten die Schnittstellen dennoch für den Fehlerfall so dimensioniert werden, dass sie auch den gesamten Netzverkehr alleine übertragen können.

- Des Weiteren kann keinesfalls garantiert werden, dass die jeweilige aktive Firewall nur die Server schützt, die sich auf dem gleichen Host-System befinden. Die virtuellen Maschinen des geschützten Netzbereichs befinden sich im gleichen Servernetz und ihre physische Lokation unterliegt weiterhin den genannten dynamischen Prozessen.

- Besteht das Host-System aus mehr als 2 Cluster-Knoten und erstreckt sich der von den virtuellen Firewalls geschützte Server-Bereich ebenfalls über mehr als 2 Knoten, kommt es zwangsläufig zu Host-System-übergreifender Netzkommunikation über die Querverbindungen der virtuellen Server Switches.

Der Active/Active-Betrieb der virtuellen Firewalls bringt dem gegenüber die gleichen Nachteile mit sich, wie sie auch von physischen Firewalls her bekannt sind: die Komplexität steigt dadurch, dass sitzungsspezifische Informationen wechselseitig ausgetauscht werden müssen. Die Kommunikationswege sind nicht mehr deterministisch und der Antwortweg einer Sitzung kann sich vom Pfad der Anfrage unterscheiden. Insofern wird auch im virtuellen Umfeld ein Active/Active-Betrieb von Firewalls nicht empfohlen.

### 4.4 Virtuelle Firewalls auf Host-System-Clustern aus mehr als 2 Knoten

Besteht die physische Server-Umgebung aus mehr als zwei Host-Systemen ist nicht nur die Konfiguration der virtuellen Switches überall einheitlich vorzunehmen, sondern auch überall eine Verbindung der virtuellen Switches erforderlich, die zum gleichen VM-Servernetz gehören. Dies mag den Einsatz zusätzlicher physischer Switches erforderlich machen, die diese Verbindungen pro virtuellem Server-Switch-Typ aufnehmen. Wie aus Abbildung 10 hervorgeht, wird die Netztopologie durch diese Firewall-Architektur und die ggf. zusätzlichen Layer-2-Switches deutlich verkompliziert.

## 5. Management der virtualisierten Umgebung

An dieser Stelle kommt eine weitere Herausforderung ins Spiel: das Management dieser virtualisierten Umgebung. Während das Managementsystem für die virtuellen Firewalls identisch mit demjenigen für physische Firewalls ist und für die virtuellen Maschinen ebenfalls leistungsfähige Managementsysteme als Teil der Virtualisierungslösung erhältlich sind, gibt es derzeit kein Werkzeug, mit dem das entstandene Datennetz einheitlich und über-

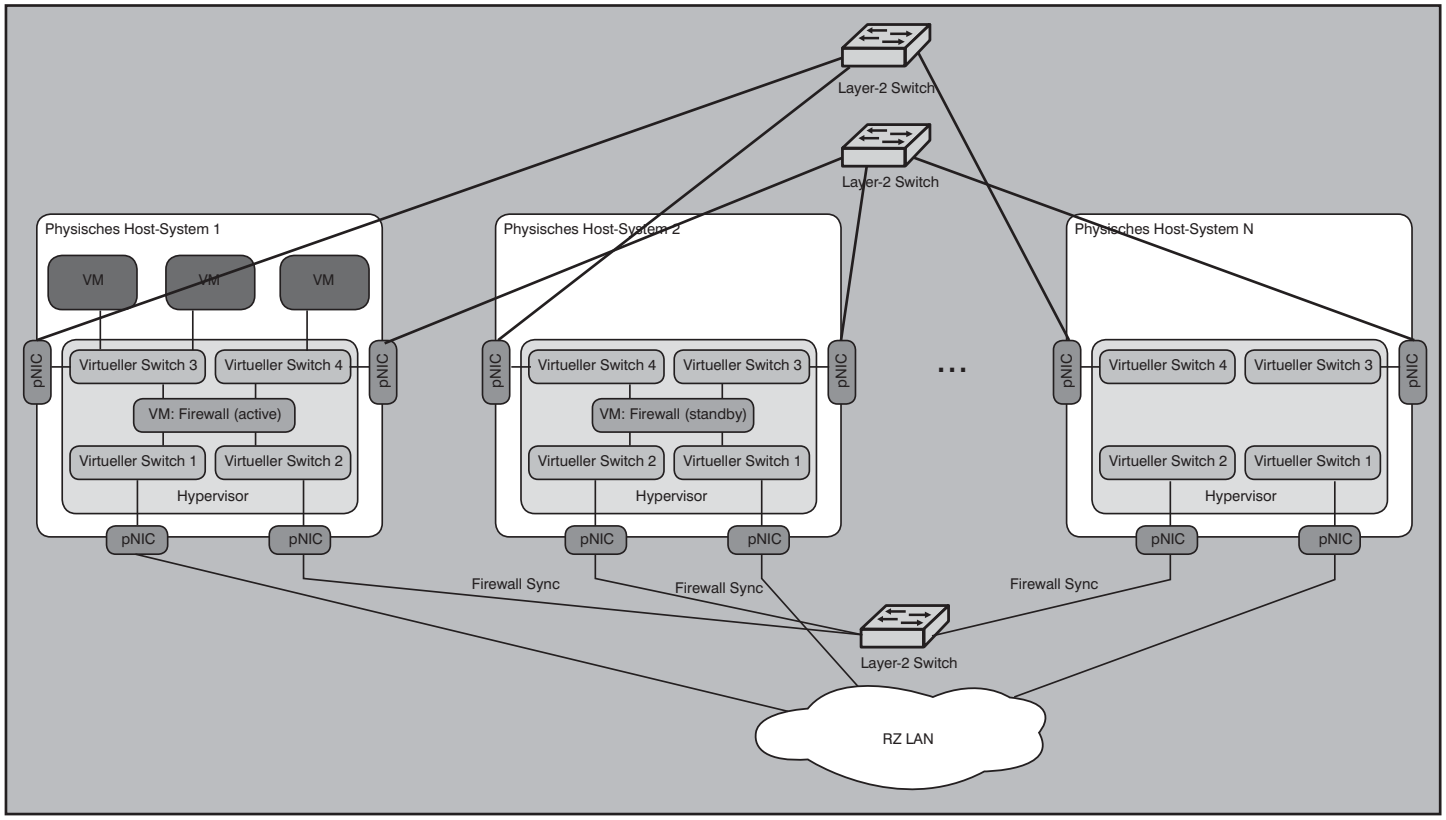



Abbildung 10: Bei mehr als 2 physischen Host-Systemen werden zusätzliche Layer-2 Switches erforderlich, die die zusammengehörenden virtuellen Server Switches sowie die Switches für den Firewall Sync mit einander verbinden.

sichtlich administriert werden könnte.

Abbildung 11 stellt das Beispiel einer logischen Darstellung der Netzwerktopologie innerhalb eines Host-Systems inkl. virtueller Firewall ihrer Repräsentation im VMware Managementsystem „Virtual Center“ gegenüber. Weder der Zusammenhang zwischen den virtuellen Switches noch die Tatsache, dass es sich jeweils um die gleiche virtuelle Firewall an den virtuellen Switches handelt, wird deutlich. Hier ist dringend eine übergreifende Managementlösung gefragt, die sowohl das physische als auch das virtuelle Netzwerk inkl. virtueller Netzkomponenten einheitlich darstellt.

Da die Virtualisierung von Servern als ein wesentliches Ziel die optimierte Ausnutzung von physikalischen Ressourcen hat, gehören Mechanismen zu der Virtualisierungslösung, die die Verlagerung einzelner virtueller Maschinen auf andere Server im laufenden Betrieb ermöglichen. Schon bei Verwendung von getrennt betriebenen Sicherheitskomponenten stellt dieses Verhalten eine Herausforderung für die Sicherheit dar. Bei jeder Bewegung der virtuellen Maschinen von einem physischen Server zum nächsten muss sichergestellt sein, dass die virtuelle Maschine nach Umzug wieder im gleichen Sicherheitskontext zu finden ist. Dies ist jedoch weniger eine technische, als vielmehr eine menschliche Herausforderung, da hier die Auswirkungen von versehentlich falscher Konfiguration den Server in das falsche VLAN und damit auch in den falschen Sicherheitskontext setzen kann. Auch an dieser Stelle ist also eine ganzheitliche, übersichtliche Managementumgebung gefragt.

### 6. Verteilte virtuelle Switches

Im vorangehenden Abschnitt wurde dargestellt, dass für Umzüge von virtuellen Maschinen im laufenden Betrieb und für eine konsistente Integration redundanter virtueller Firewalls die gleiche Netztopologie in den Host-Systemen vorliegen muss. Da die Managementsysteme der gängigen Virtualisierungslösungen in dieser Hinsicht wenig Transparenz bieten, ist der manuelle Weg dieser Konfiguration bei zahlreichen Hosts nicht nur sehr aufwendig, sondern auch äußerst fehlerträchtig. Abhilfe schaffen kann hierbei z.B. eine Skript-gesteuerte Konfiguration der virtuellen Switches.

VMware bietet mit dem unter dem Namen „vSphere 4“ erschienenen neuen Release seiner Virtualisierungslösung sogenannte „Distributed Virtual Switches“ an, um diesem Problem zu begegnen. Die Idee hierbei ist, dass nicht mehr einzelne virtuelle Switches je Host-System konfiguriert werden müssen, sondern dass sich die virtuellen Switches über den gesamten Host-System-Cluster erstrecken. Abbildung 12 zeigt, wie sich zumindest die logische Darstellung dieser Architektur inkl. virtueller Firewalls dadurch vereinfacht. Es bleibt jedoch fraglich, ob diese verteilten virtuellen Switches aus mehr als einem Perl-Skript bestehen, die deren Konfiguration auf allen Host-Systemen vereinheitlichen. So ist z.B. unklar, ob in diesem Konzept die Kommunikation zwischen den einzelnen virtuellen Switch-Segmenten, die sich auf unterschiedlichen Hosts befinden, aber dem gleichen verteilten virtuellen Switch zugeordnet sind, vorgesehen ist und über welche physischen Verbindungen dieser Da-

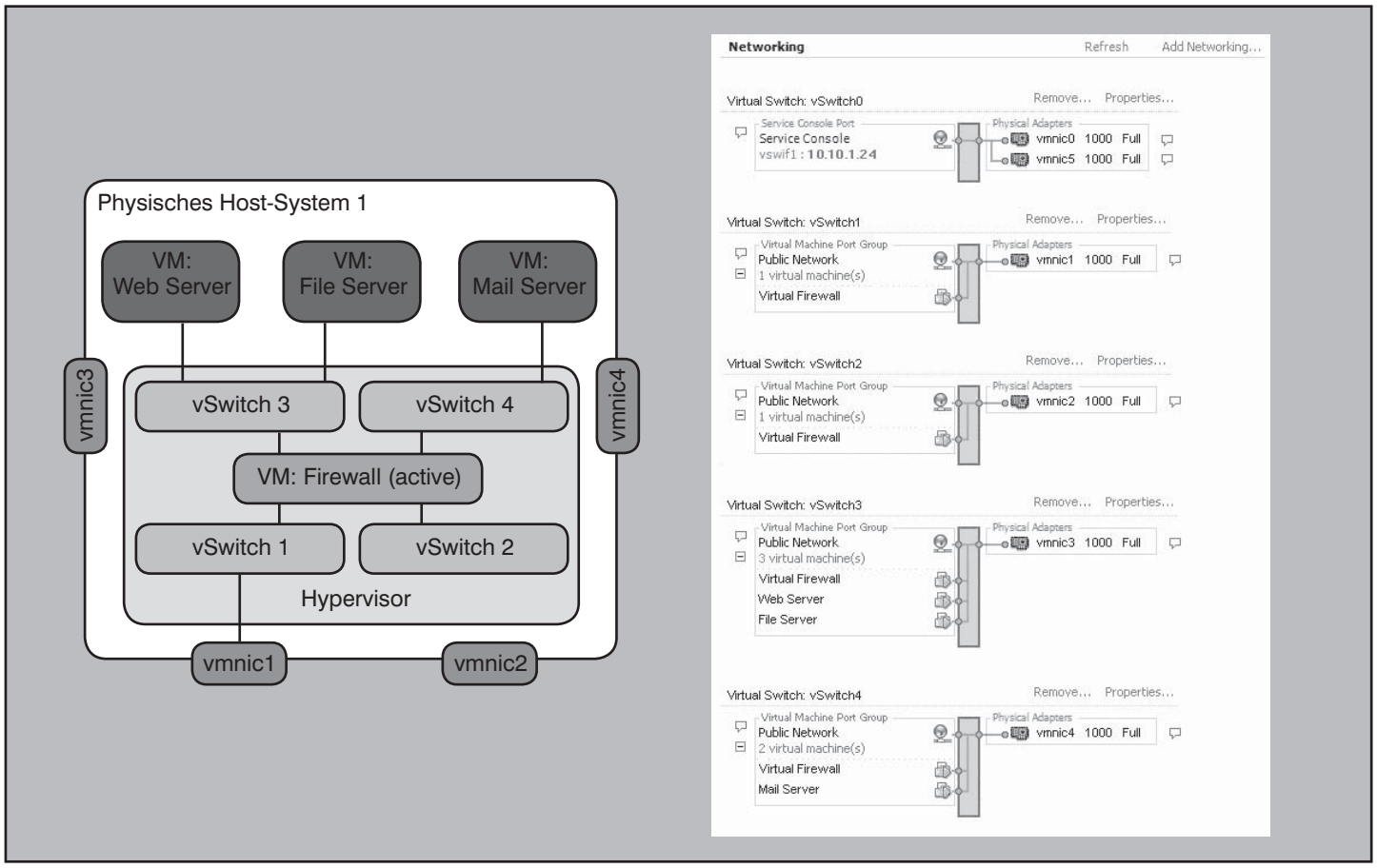



Abbildung 11: Logische Darstellung der virtuellen Netztopologie eines Host-Systems inkl. virtueller Firewall (links) und die Darstellung in der VMware Managementumgebung Virtual Center (rechts).

tenverkehr dann stattfindet (vgl. z.B. die dedizierte Verbindungen zwischen den virtuellen Switches 4 beider Hosts in Abbildung 7). Gerade im Failover-Fall der virtuellen Firewall oder beim Verschieben von virtuellen Maschinen kommt der Beantwortung dieser Frage auch in dieser Architektur eine hohe Bedeutung zu.

### 7. Technische Einschränkungen beim Einsatz von virtuellen Firewalls

Betrachtet man die Umstände, die mit der Virtualisierung von Firewalls einhergehen, genauer, zeigen sich auch technische Einschränkungen, die mit diesem Ansatz einhergehen. Zunächst sei herausgestellt, dass einer virtuellen Firewall in der Regel nicht dediziert die Gesamtleistung des Host-Systems zur Verfügung steht, wie es bei einer physischen Appliance der Fall ist. Die Firewall muss sich die verfügbare Hardware-Leistung wie beispielsweise CPU, RAM und Netzwerkdurchsatz mit den anderen virtuellen Maschinen teilen. Damit ist klar, dass eine virtuelle Firewall nur dann die gleiche Leistung bringen kann wie die gleiche Software auf einer Appliance, wenn – neben der identischen Hardware-Basis – bis zu 100% der Ressourcen von der Firewall beansprucht werden dürfen.

Ab einer gewissen zu erwartenden Durchschnittslast, die von der virtuellen Firewall verursacht wird, widerspricht es allerdings dem ursprünglichen Virtualisierungsgedanken – nämlich eine möglichst hohe Konsolidierungsrate zu erzielen –, wenn virtuelle Firewall und virtuelle Server auf dem gleichen Host-System betrieben werden. Müssen z.B. 50% der Host-Ressourcen der virtuellen Firewall zur Verfügung stehen, können nur noch halb so viele virtuelle Server auf diesem Host betrieben werden, als wenn man die Firewall als dedizierte physische Appliance realisiert hätte.

Abhängig von den weiteren virtuellen Maschinen, die auf dem physischen System betrieben werden, ergeben sich außerdem schwer vorhersehbare Lastprofile für die Performance. Dies führt zu einer weiteren Beschränkung des Einsatzbereiches einer virtuellen Firewall gegenüber ihrem physischen Pendant. So wird klar, dass eine Virtualisierung der Firewall umso weniger erstrebenswert ist, je größer ihre eigenen Leistungsanforderungen sind.

Die Virtualisierung setzt letztlich auf einem Stück Software, dem Hypervisor, auf. Sicherheitsschwächen im Hypervisor betreffen somit auch unweigerlich alle virtuellen Systeme und daher ebenso die virtuelle Firewall. Gerade an Sicherheitskomponenten bestehen in der Regel besondere Anforderungen hinsichtlich ihres Betriebs in einer gehärteten Umgebung. Diese Tatsache ist daher in die Entscheidung für oder gegen eine virtuelle Firewall mit einzubeziehen.

Um einem virtuellen Gesamtsystem umfassenden Schutz zu geben, reicht daher eine virtuelle Firewall, die wie ein weiterer virtueller Server einfach an den virtuellen Switch gebunden wird, oftmals nicht aus. Vielmehr muss es einen Schutzmechanismus geben, der tiefer in die virtuelle Infrastruktur eingreift.

#### 7.1 VMsafe

Der Hersteller VMware hat die genannten Grenzen von virtuellen Firewalls zum An-

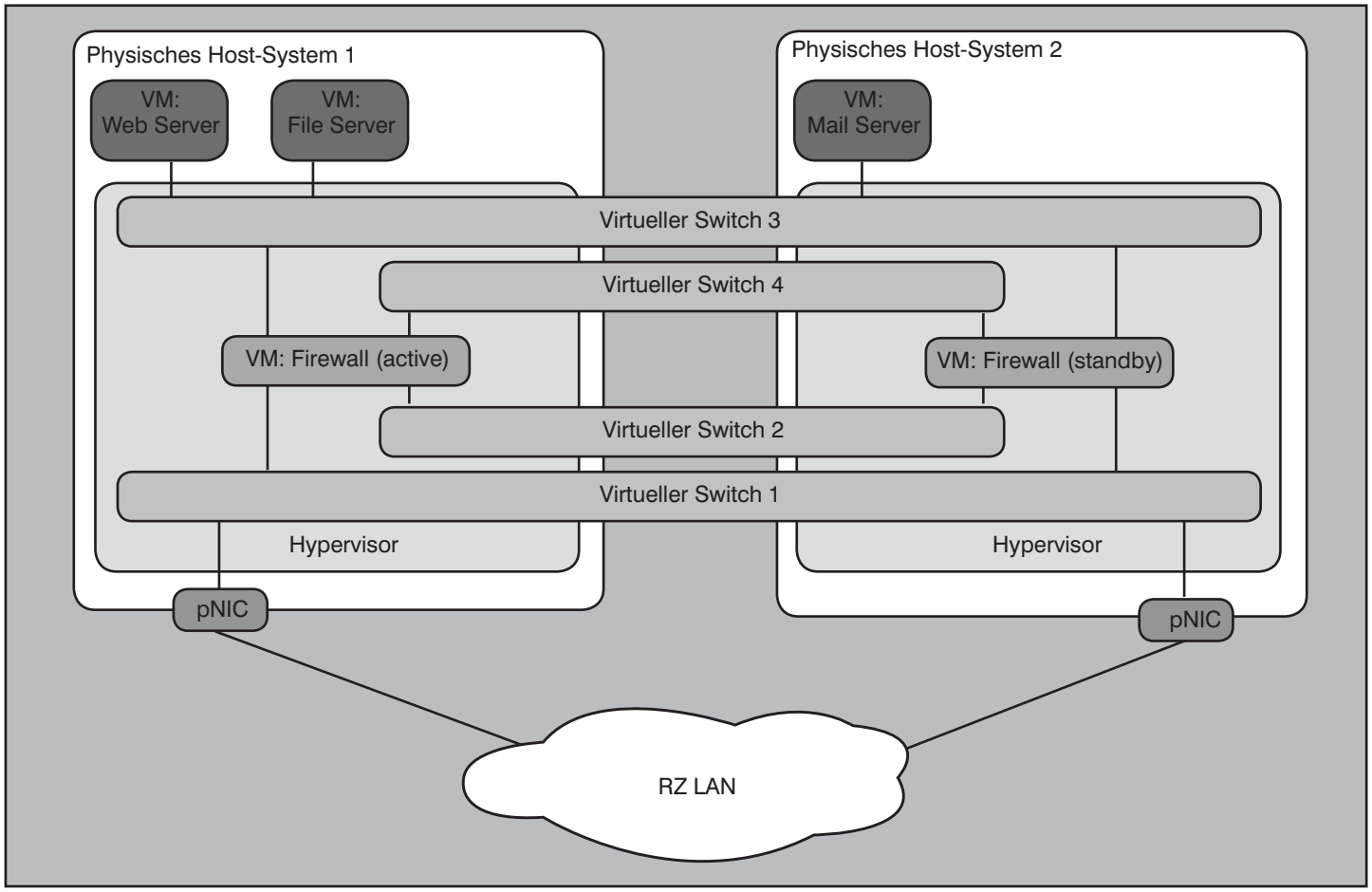



Abbildung 12: Logische Netztopologie von zwei Host-Systemen mit virtuellen Firewalls bei Einsatz von verteilten virtuellen Switches

lass genommen, die Thematik der Bildung von Sicherheitszonen zu überarbeiten. Mit der aktuellen Version vSphere 4.0 als Nachfolger von Virtual Infrastructure 3 stehen zwei Neuerungen an, welche insbesondere in Hinblick auf virtuelle Firewalls relevant sind: VMware vShield Zones und VMware VMsafe.

VMware VMsafe stellt eine Schnittstelle innerhalb des VMware Hypervisors dar, über welche der Zugriff auf CPU, Arbeitsspeicher, Massenspeicher und Netzwerk der virtuellen Maschinen erfolgen kann. Im Gegensatz zu bisherigen virtuellen Firewall-Produkten, welche in der Regel nur aus der Firewall-Software in einer virtuellen Maschine anstatt auf physischer Hardware bestehen, berücksichtigt diese Schnittstelle Spezifika der Virtualisierung. Der Zugriff der VMsafe-kompatiblen Systeme (z.B. einer virtuellen Firewall) erfolgt vollkommen transparent, d.h. eine Änderung der virtuellen Netztopologie ist nicht erforderlich.

Dies erlaubt u.a. folgende Einsatzmöglichkeiten:

- Erkennung von schadenstiftender Software ohne Installation eines separaten Agenten.

  Hierdurch ist z.B. eine zentrale Anti-Virus-Erkennung mittels einer VMsafe-kompatiblen VM anstatt der Installation eines Agenten in jeder VM möglich. Dies schont zum einen die Ressourcen, zum anderen kann auf diese Weise keine Schadsoftware den Agenten innerhalb der VM deaktivieren.

- Kontrolle des ein- und ausgehenden Netzverkehrs mittels Paketfilter/ IDS/ IPS

  Auf Basis eines dynamischen Paketfilters kann ein- und ausgehender Verkehr virtueller Maschinen kontrolliert werden. Aber auch eine Spiegelung des Verkehrs einzelner TCP/IP-Ports auf ein externes System ist möglich. Ein Beispiel ist die Spiegelung von HTTP-Verkehr auf ein IDS-System zur weiteren Analyse. Die Regeln können dabei auf verschiedenen Ebenen greifen. Auf Basis einer VM, einer Gruppe von VMs oder global. So könnte beispielsweise eine globale Standardregel für alle VMs lauten, dass eingehender Verkehr blockiert wird. Ebenso lassen sich IDS/IPS-Systeme transparent in die virtuelle Infrastruktur einbinden.

Auf der anderen Seite gibt es auch Kritikpunkte bezüglich VMsafe:

- Der Zugriff auf die Schnittstelle wird von VMware kontrolliert. Im Rahmen eines Review-Prozesses muss der potentielle Partner Details zur Verwendung und seine Absichten darlegen. Letztendlich entscheidet VMware, ob dieser zur Nutzung berechtigt ist. Dem gegenüber bieten offene Schnittstellen wie etwa unter XenServer deutliche Vorteile.

- Die Integration zusätzlicher Funktionalität in den Hypervisor erhöht das Risiko von Softwarefehlern und damit die Gefahr von Schwachstellen. Die erfolgreiche Kompromittierung der VMsafe-Schnittstelle entspricht prinzipiell der Kompromittierung des Gesamtsystems.

Generell erfordert die VMsafe API jedoch entsprechende Neuentwicklungen von Produkten, damit diese die neuen Funktionen auch nutzen können.

### 7.2 VMware vShield Zones

Eine weitere Option für Kunden und Hersteller ist die Nutzung von VMware vShield Zones.

Mittels der Software-Option VMware vShield Zones (ab vSphere Advanced Edition) ist es innerhalb der virtuellen Umgebung möglich, verschiedene Sicherheitszonen zu bilden. Die Grundlage hierfür bildete das Produkt VirtualShield der Firma Blue Lane, welche VMware 2008 übernommen hat. Über eine separate VM (vShield Zones VA) je physischem Server und eine Management-VM (vShield Zones Manager) können verschiedene Sicherheitszonen auf Basis einer gemeinsamen physischen Infrastruktur gebildet werden. Dies ermöglicht beispielsweise das Erstellen von Firewall-Regeln je VM, Switch oder Cluster. Ebenso wird der Sicherheitskontext einer VM bei Nutzung von z.B. vMotion beibehalten. Die Konfiguration und das Management sind hierbei in die VMware-Management-Werkzeuge (vCenter Server) integriert. Derzeit befinden sich die vShield Zones noch in einer privaten Betaphase, so dass derzeit keine detaillierten Infos oder Erfahrungswerte diesbezüglich vorliegen.

### 8. Tests

Wie für die gesamte Virtualisierungstechnologie gilt auch und gerade für den Sicherheitsbereich, dass ausgiebige Tests unerlässlich sind. Während virtualisierte Firewalls bereits vielfältig erfolgreich genutzt werden und ihr Einsatz nur geringen Einfluss auf die Kommunikationsflüsse hat, müssen beim Einsatz von virtuellen Firewalls die dynamischen Prozesse der virtuellen Umgebung ausgiebig untersucht werden.

Des Weiteren ist das Lastverhalten der virtuellen Firewall in einer Testumgebung mit möglichst realistischen Datenaufkommen zu analysieren. Anhand der von der Firewall angeforderten Systemressourcen ist zu entscheiden, ob eine virtuelle Lösung dienlich ist.

### 9. Fazit und Ausblick

Die Verwendung von virtuellen Firewalls hat insbesondere beim redundanten Einsatz enormen Einfluss auf die logische Netztopologie und die Verkehrsflüsse innerhalb einer virtualisierten Umgebung. Die marktgängigen Managementlösungen bieten derzeit noch keine ausreichende Unterstützung, um das physische und

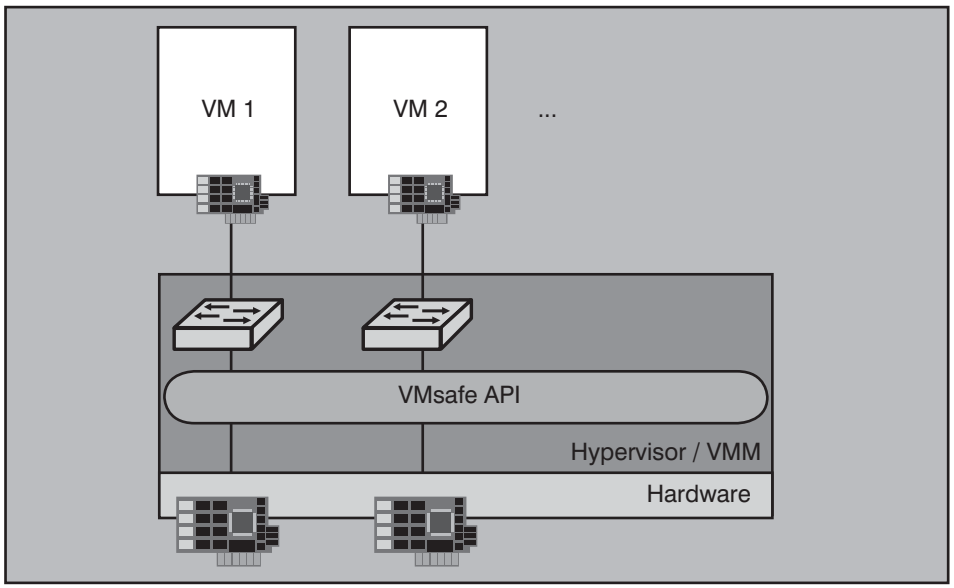



Abbildung 13: VMsafe API innerhalb des VMware Hypervisors

virtuelle Netzwerk sowie die darin befindlichen virtuellen Sicherheitskomponenten ganzheitlich zu überwachen und somit für das erforderliche Sicherheitsniveau des Gesamtsystems zu sorgen.

Insofern ist die Eignung virtueller Firewalls für die Segmentierung eines Rechenzentrumnetzes in unterschiedliche Sicherheitszonen als fraglich zu betrachten. Ihr Einsatz ist eher prädestiniert, um einzelnen Serversystemen, die nur eine eingeschränkte Dynamik besitzen, einen zusätzlichen Schutz zu bieten.

Für darüber hinaus gehende Anforderungen sind neue Konzepte gefragt. Ob diese in Form von VMwares VMsafe API und den vShield Zones realisiert werden, bleibt bei Verfügbarkeit dieser Produktmerkmale näher zu untersuchen.

## 10. Abkürzungen

| | |
|---|---|
| API | Application Programming Interface |
| ARP | Address Resolution Protocol |
| ASIC | Application Specific Integrated Circuit |
| CPU | Central Processing Unit |
| DMZ | Demilitarized Zone, Demilitarisierte Zone |
| DRS | Distributed Ressource Scheduler |
| HA | High Availability |
| HBA | Host Bus Adapter |
| HTTP | Hypertext Transfer Protocol |
| IDS | Intrusion Detection System |
| I/O | Input / Output |
| IP | Internet Protocol |
| IPS | Intrusion Prevention System |
| iSCSI | internet Small Computer System Interface |
| LAN | Local Area Network |
| MAC | Media Access Control |
| NIC | Network Interface Card |
| OSI | Open Systems Interconnection |
| OVF | Open Virtual File Format |
| pNIC | physical NIC |
| QoS | Quality of Service |
| RAM | Random Access Memory |
| RZ | Rechenzentrum |
| STP | Spanning Tree Protocol |
| TCP | Transmission Control Protocol |
| UTM | Unified Threat Management |
| VHD | Virtual Hard Disk |
| VLAN | Virtual LAN |
| vNIC | virtual NIC |
| VM | Virtual Machine, Virtuelle Maschine |
| VMDK | Virtual Machine Disk Format |
| VPN | Virtual Private Network |

ComConsult Veranstaltungskalender

# Aktuelle Veranstaltungen

### Sonderveranstaltung: Netzwerk-Design-Wettbewerb 2009, 25.05. - 26.05.09 in Köln

Alcatel-Lucent, Brocade/Foundry, Cisco, Enterasys, Extreme, H3C/3com, HP, Juniper und Nortel stellen sich dem Vergleich. Basierend auf einem realisitischen Projekt-Szenario in Form eines RFI (Request for Information in der Anlage) haben die Hersteller detaillierte Planungen für das Szenario entworfen und umfangreiche Funktionslisten für alle angebotenen Produkte bearbeitet. Die Ergebnisse zeigen deutliche Unterschiede zwischen den Herstellern und erlauben die Beantwortung der Frage: wo steht mein bisheriger Hersteller mit seinen Produkten, bieten andere Hersteller ggf eine sinnvolle Alternative, bietet eine Kombination zweier Hersteller im Sinn einer Dual Vendor Strategie Vorteile?

Preis: € 1.690,- zzgl. MwSt.

### TCP/IP und SNMP, 25.05. - 29.05.09 in Aachen

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

Preis: € 2.290,- zzgl. MwSt.

### Wireless LAN professionell, 25.05. - 27.05.09 in Hamburg

Dieses Seminar vermittelt den aktuellen Stand der WLAN-Technik und zeigt die in der Praxis verwendeten Methoden für Aufbau, LAN-Integration, Betrieb und Optimierung von WLANs im Enterprise-Bereich auf. Die verschiedenen WLAN-Varianten werden analysiert, Markt- und Produktsituation werden bewertet, und Empfehlungen für eine optimale Auswahl werden gegeben.

Preis: € 1.390,- zzgl. MwSt.

### Projektmanagement I: Projekte erfolgreich leiten, organisieren und optimieren, 25.05. - 29.05.09 in Aachen

Dieses Seminar richtet sich an Fach- und Führungskräfte, die IT-Projekte abwickeln oder sich auf die Übernahme der Projektleitung von IT-Projekten vorbereiten.

Preis: € 2.290,- zzgl. MwSt.

### Unified Communications mit Siemens - HiPath 8000 & OpenScape im Überblick, 25.05. - 26.05.09 in Hamburg

Dieses Seminar richtet sich an Fach- und Führungskräfte, die IT-Projekte abwickeln oder sich auf die Übernahme der Projektleitung von IT-Projekten vorbereiten.

Preis: € 1.390,- zzgl. MwSt.

### IP-Telefonie und Unified Communications erfolgreich planen und umsetzen, 27.05. - 29.05.09 in Köln

Das Seminar richtet sich an die Verantwortlichen, Entscheidungsträger, Planer und Betreiber von und IP-Netzwerken, TK-Anlagen und Call Centern, die sich über die optimale und erfolgreiche Weiterentwicklung bestehender klassischer oder IP-basierter TK-Lösungen informieren wollen.

Preis: € 1.690,- zzgl. MwSt.

### Sicherheit im LAN mit IEEE 802.1X, 15.06. - 16.06.09 in Stuttgart

Dieses 2-tägige Seminar vermittelt den optimalen Umgang mit IEEE 802.1X, erläutert die Einsatzvarianten, beschreibt die gegebenen Fallstricke und liefert die ideale Basis zur Vorbereitung eines Einsatzes.

Preis: € 1.390,- zzgl. MwSt.

### Office Communications Server 2007 R2, 15.06. - 16.06.09 in Stuttgart

Das Seminar richtet sich in erster Linie an IT-Entscheider, die einen detaillierteren Blick in den OCS werfen wollen, sowie Administratoren, die einen ersten etwas tieferen Blick in die Thematik wünschen.

Preis: € 1.390,- zzgl. MwSt.

### SIP (Session Initiation Protocol ) - Basis-Technologie der IP-Telefonie, 15.06. - 17.06.09 in Stuttgart

Das Seminar richtet sich an die Verantwortlichen, Entscheidungsträger, Planer und Betreiber von TK-, VoIP-, UC-Lösungen und Call Centern, die sich über die optimale und erfolgreiche Weiterentwicklung bestehender Telefonie-Lösungen in Richtung SIP informieren wollen.

Preis: € 1.690,- zzgl. MwSt.

### IP-Telefonie: Vorbereitung, Migration, Management, 15.06. - 17.06.09 in Stuttgart

Dieses Seminar richtet sich an die Verantwortlichen für die Planung und Einführung von IP-Telefonieumgebungen. Grundkenntnisse in Netzen und Telefonie werden vorausgesetzt.

Preis: € 1.690,- zzgl. MwSt.

### Sicherheit 3: Zur erfolgreichen Konfiguration von Firewalls, VPNs, Windows Clients und WLANs, 15.06. - 19.06.09 in Aachen

Dieses einmalige Seminar vermittelt intensiv innerhalb von 5 Tagen den praktischen Umgang mit Firewalls, VPNs, Windows-Sicherheit und WLAN-Sicherheit. Im Rahmen von praktischen Live-Übungen werden typische Konfigurationen analysiert und vermittelt.

Preis: € 2.290,- zzgl. MwSt.

Zertifizierungen

## ComConsult Certified Network Engineer

**Lokale Netze**
**11.05. - 15.05.09 in Aachen**
**31.08. - 04.09.09 in Frankfurt**
**23.11. - 27.11.09 in Hamburg**

**TCP/IP und SNMP**
**25.05. - 29.05.09 in Aachen**
**21.09. - 25.09.09 in Bonn**

**Internetworking**
**11.05. - 15.05.09 in Aachen**
**05.10. - 09.10.09 in Frankfurt**

Paketpreis für alle drei Seminare € 6.183,-- zzgl. MwSt. (Einzelpreise: je € 2.290.--)

## ComConsult Certified Trouble Shooter

**Trouble Shooting 1**
**06.10. - 09.10.09 in Aachen**

**Trouble Shooting 2**
**23.06. - 26.06.09 in Aachen**
**03.11. - 06.11.09 in Aachen**

Paketpreis für beide Seminare, eine digitale Stromzange, die Prüfung und den Report „Fehlersuche in konvergenten Netzen“ € 3.940.-- zzgl. MwSt.
(Einzelpreise: je € 2.190.--)

## ComConsult Certified Security Expert

**Sicherheit 1: Grundlagen und Kernbausteine zur erfolgreichen IT-Sicherheit**
**14.09. - 18.09.09 in Köln**

**Sicherheit 2: Erarbeitung und Umsetzung von Sicherheitskonzepten**
**26.10. - 30.10.09 in Aachen**

**Sicherheit 3: Praxis-Intensiv-Seminar zur erfolgreichen Konfiguration von Firewalls, VPNs, Windows Clients und WLANs**
**15.06. - 19.06.09 in Aachen**
**23.11. - 27.11.09 in Aachen**

Paketpreis für alle drei Seminare und die beiden Reports „VPN-Technologien: Alternativen und Bausteine einer erfolgreichen Lösung“ und „Sicherheit in Wireless LANs“. € 6.183.-- zzgl. MwSt. (Einzelpreise: je € 2.290.--)

## ComConsult Certified Voice Engineer

**Basis-Seminar: Session Initiation Protocol-Basis-Technologie der IP-Telefonie**
**15.06. - 17.06.09 in Stuttgart**
**28.09. - 30.09.09 in Bad Neuenahr**
**23.11. - 25.11.09 in Hamburg**

**Basis-Seminar: Sicherheitsmechanismen für Voice over IP**
**12.05. - 13.05.09 in Bonn**
**05.10. - 06.10.09 in Frankfurt**

**Alternative 1: IP-Telefonie und Unified Communications erfolgreich planen und umsetzen**
**27.05. - 29.05.09 in Köln**
**14.09. - 16.09.09 in Köln**
**02.11. - 04.11.09 in Frankfurt**

**Alternative 2: IP-Telefonie: Vorbereitung, Migration, Management**
**15.06. - 17.06.09 in Stuttgart**
**26.10. - 28.10.09 in Berlin**

**Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter**
**07.09. - 08.09.09 in Aachen**
**09.11. - 10.11.09 in Königswinter**

Basis-Paket Alternative 1: Beinhaltet die zwei Basis-Seminare und Seminar „Alternative 1“
Grundpreis: € 4.250,-- zzgl. MwSt. statt € 4.770,-- zzgl. MwSt.

Basis-Paket Alternative 2: Beinhaltet die zwei Basis-Seminare und Seminar „Alternative 2“
Grundpreis: € 4.250,-- zzgl. MwSt. statt € 4.770,-- zzgl. MwSt.

Optionales Einsteigerseminar: Aufpreis € 990,-- zzgl. MwSt. statt € 1.390,-- zzgl. MwSt.

Impressum

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

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

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

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