ComConsult Research

Der Netzwerk Insider

März 2009

Systematische Weiterbildung für Netzwerk- und IT-Professionals

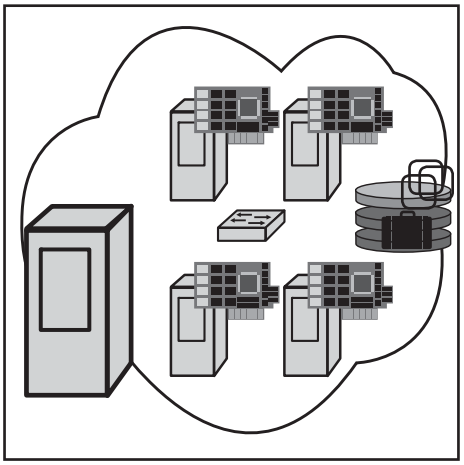
Schwerpunktthema

Virtualisierung: Sicherheit in virtuellen Server-Umgebungen

von Dipl.-Inform. Oliver Flüs, Dr. Simon Hoff, Dipl.-Inform. Daniel Meinhold

Mit dem Einsatz von Server-Virtualisierung sind konkrete Erwartungen an eine verbesserte Wirtschaftlichkeit der IT verbunden:

- **Kosteneinsparungen durch Reduzierung der Hardware-Kosten für Server**
- **Einfacheres Management durch vereinheitlichte Infrastruktur**
- **Erhöhte Verfügbarkeit durch High-Availability-Konzepte mit minimierter Hardware-Abhängigkeit, neue Optionen bzgl. Behandlung von Notfällen im Server-Bereich**
- **Steigerung der Effizienz und Qualität durch vereinfachte Test- und Entwicklungsumgebungen**



Im Rahmen dieses Artikels werden die betroffenen technischen Kernkomponenten und deren Zusammenspiel in Bezug auf die IT-Sicherheit betrachtet. Neben potentiellen Gefährdungen sowie möglichen Maßnahmen wird hierbei auch auf veränderte IT-Betriebs- und Geschäftsprozesse hingewiesen, denn mit der Einführung der Virtualisierung ergeben sich weitreichende Änderungen, die nicht nur den Server-Betrieb betreffen.

weiter auf Seite 23

Zweitthema

IT-Verkabelung im Rechenzentrum: Beginn einer neuen Epoche?

von Dipl.-Inform. Hartmut Kell

Bis vor einigen Jahren gab es lediglich eine Vorstellung wie eine Verkabelung im Bereich des Endgeräteanschlusses und im Bereich der Verteilerverbindungen auszusehen hat. Mitte der 90er Jahre wurden die Grundsteine für Standardisierungen dieser Technik gelegt und diese bis heute weiterentwickelt. Vernachlässigt wurde in all dieser Zeit der Bereich des Rechenzentrums bzw. der Server-Räume.

Das Ergebnis lässt ist bei Eintritt in viele Rechenzentren ersichtlich, eine bedarfsorientierte, ohne Konzept realisierte und im Laufe der Jahre zunehmend chaotisch gewordene passive IT-Infrastruktur. Dieses Chaos wird weiter verschärft durch - trotz Einführung von VM-Lösungen - zunehmende Anzahl von Servern mit zum Teil sehr unterschiedlichen Anforderungen an die Übertragungstechnik oder -art der notwendigen LAN-Schnittstellen.

Sowohl bei Aufbau von neuen Rechenzentren wie auch beim Redesign von vorhandenen Rechenzentren ist es an der Zeit, über bisher praktizierte Techniken und alternative Möglichkeiten nachzudenken. Der nachfolgende Artikel wird sich mit diesen Alternativen beschäftigen und dabei versuchen, abseits der Pfade der Hersteller nach „immer schneller und immer besser“ Wege zu beschreiben, die Praxisnah und realistisch bleiben.

weiter auf Seite 10

Neue Kongresse

OCS-Forum 2009

IT-Sicherheits-Forum 2009

ab Seite 4

Geleit

ComConsult OCS-Forum 2009: muss das sein?

ab Seite 2

Neues Seminar

Unified Communications mit Siemens - HiPath 8000 & OpenScape im Überblick

ab Seite 22

Zum Geleit

ComConsult OCS-Forum 2009: muss das sein?

Nach der Ankündigung des ComConsult OCS-Forums sind eine Reihe von Fragen an uns heran getragen worden. Dazu die folgenden Anmerkungen:

- das OCS-Forum 2009 wird sich nicht nur mit dem Microsoft Office Communications Server befassen, sondern bewusst auch die verfügbaren Lösungen anderer Hersteller gegenüber stellen und die Vor- und Nachteile der einzelnen Ansätze bewerten

- Microsoft OCS befindet sich in einer zentralen Sonderrolle im Markt, wir werden das nachfolgend erklären. Im Kern steht die Erwartung, dass viele Microsoft-Kunden, die auch mit Exchange, Office und Sharepoint arbeiten, OCS als natürliche Ergänzung des Portfolios nutzen werden (und dabei ggf. auch lizenztechnische Vorteile haben werden)

Tatsache ist, dass viele Unternehmen Microsoft OCS im Moment evaluieren und auch die führenden TK-Hersteller OCS offenbar als gegeben ansehen und sich entsprechend um die Integration bzw Kopplung bemühen.

Tatsächlich steht hinter der ganzen emotionalen und kontroversen Diskussion die Frage nach der richtigen Strategie im Übergang zu Unified Communications oder allgemeiner zur IP-Sprach-/Video- und Multimedia-Kommunikation.

Dazu einige Thesen, die die Problematik der Erarbeitung einer optimalen Strategie für ein bestehendes Unternehmen erläutern:

These 1:
Unified Communications als Synonym für moderne IP-Telefonie ist die Zukunft. Die Frage ist nicht ob, sondern wann und wie viel.

These 2:
Das Grundproblem aller Migrationen nach IP-Telefonie oder Unified Communications sind die sehr unterschiedlichen Anforderungen der verschiedenen Teilnehmergruppen in den Unternehmen. So werden zu Beginn der Projekte in den meisten Unternehmen nur kleine Teilnehmergruppen den vollen Funktionsumfang der neuen Kollaborations-Werkzeuge nutzen. Damit entsteht die Frage, ob es wirtschaftlich ist, eine flächendeckende Installation von UC zu starten.

These 3:
In Anlehnung an These 2 entsteht die Kernfrage aller aktuellen Projekte in diesem Bereich: sofort komplett umsteigen oder stufenweise langsam migrieren? Dabei darf nicht der Fehler begangen werden, dies als reine Kostenfrage zu sehen. Unified Communications schafft auch eine neue Kommunikationsfunktionalität. Diese wiederum verbessert die Effizienz der Kommunikation und schafft wirtschaftliche Werte.

These 4:
Für alle Kunden, die nicht auf einen Schlag umsteigen wollen, wird Microsoft OCS einen erheblichen Reiz haben. Die Botschaft ist klar: die bestehende TK-Anlage kann behalten werden und OCS liefert alle neuen Funktionen (und würde ggf. sowieso eingeführt werden, um Sharepoint und Exchange zu ergänzen). Es muss auch klar sein, dass ein sofortiger Komplettumstieg mit OCS nicht geht.

These 5:
Stufenweise Migrationen sind mit äußerster Vorsicht zu genießen. Auch wenn sie auf den ersten Blick attraktiv sind, so haben sie nicht nur die Kosten-Nachteile des Parallelbetriebs zweier Systeme. Wie immer in solchen Architekturen müssen Gateways eingesetzt werden. Auch wenn diese jetzt Mediation Server heißen und einen schöneren Namen haben, bleiben es Gateways mit allen Problemen der Abbildung ggf. inkompatibler Leistungsmerkmale aufeinander. Im Falle von Microsoft OCS ist es noch komplexer. So hat Microsoft ein sehr spezielles Verständnis von Teilnehmern und dieses weicht ggf. von dem traditionellen Teilnehmer-Verständnis auf der TK-Seite ab.

These 6:
OCS ist eine interessante Bereicherung des Marktes. Doch es darf nicht der Fehler begangen werden, dies als eine Übergangs-Lösung anzusehen. Wer OCS einführt, der sollte auch die Langfrist-Option sehen, dass dies die künftige Komplett-Lösung für sein Unternehmen sein wird/kann. OCS liefert einiges an Funktionalität und hat einen entsprechenden Einrichtungs-Aufwand. Dieser sollte nicht als Spielerei oder Testerei angesehen werden. Entweder wird das Projekt ernsthaft und richtig aufgesetzt oder gar nicht.

These 7:
Fast alle wichtigen Hersteller haben echte Alternativen zu OCS. Dies betrifft nicht nur den Funktionsumfang, sondern auch die Architektur der Lösung. Avaya und Siemens gehen beide in Richtung virtualisierter SOA-Architekturen. Diese Art von Lösung hat auf Dauer gesehen erhebliche Vorteile, sie skaliert besser und senkt den Betriebsaufwand erheblich. Auch bietet sie die ideale Umgebung, um klein anzufangen und stufenweise zu wachsen. Eine zu schnelle Entscheidung in Richtung OCS sollte deshalb nicht getroffen werden, ohne die Alternativen zu prüfen. Die Angebote der verschiedenen Hersteller müssen sorgfältig miteinander verglichen werden, um die jeweils optimale Lösung für ein Unternehmen zu finden.

These 8:
Es besteht das ernstzunehmende Risiko, dass die Langfristkosten eines OCS-Projekts unterschätzt werden. Der Einstieg wird für einen größeren Microsoft-Bestandskunden möglicherweise sehr preiswert sein (Nutzung vorhandener Server und auch CAL´s). In jedem Fall ist eine Kalkulation der Langfristkosten dringend anzuraten.

These 9:
Microsoft OCS und die zugehörigen Client-Lösungen sind technisch interessant. Sie haben einen etwas behäbigen Markt gehörig aufgemischt und auf jeden Fall bereichert. Es bedurfte offensichtlich der

ComConsult OCS-Forum 2009: muss das sein?

Marktmacht Microsofts, um die Hersteller endlich in den Übergang zu Wideband-Codecs zu bringen und eine wirklich gute Sprachqualität umzusetzen. Auch auf der Seite der Video-Konferenz zeigt Microsoft zusammen mit Polycom und Tandberg, was heute technisch möglich ist. Speziell die Kombination aus der neuen Tandberg PrecisionHD-Kamera (erst in Q2 verfügbar) und dem Office Communicator R2 bringt endlich die lange geforderte Integration aus HD-Video im Desktop in die großen Telepresence-Systeme. Siemens folgt dieser Richtung schon seid letztem Jahr, die anderen werden ohne Frage bedingt durch die bestehende enge Zusammenarbeit mit Tandberg und Polycom kurzfristig folgen (dies gilt speziell für Avaya und Alcatel). Cisco ist damit deutlich unter Druck, seine Telepresence-Lösung endlich zu öffnen.

Wie diese Thesen zeigen, so gibt es allen Anlass, zum Thema Office Communications Server sehr unterschiedliche Sichtweisen zu haben. Microsoft hat mit diesem Produkt und der gerade erfolgten Umstellung auf Release 2 den Markt verändert.

Wir stellen uns mit dem ComConsult OCS-Forum 2009 dieser sehr kontroversen Marktsituation. Wir präsentieren aktuelle Ergebnisse unserer laufenden Analysen in diesem Bereich und zeigen auf, welche Argumente pro und kontra dieser Entwicklung zu beachten sind.

Ich habe keinen Zweifel, dass dies ein sehr spannendes Forum wird.

Ihr
Dr. Jürgen Suppan

Neuer Kongress

ComConsult OCS-Forum 2009: offene TK- und Kollaborations-Lösungen auf dem Prüfstand

Die ComConsult Akademie veranstaltet vom 04.05. - 05.05.09 ihren Kongress „ComConsult OCS-Forum 2009“ in Königswinter.

Mit der Freigabe des Release 2 des Office Communications Servers OCS stehen viele Unternehmen nun vor der Entscheidung, welchen Weg sie gehen sollen:

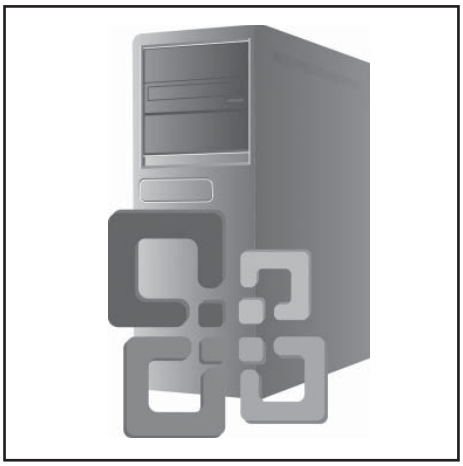
Alternative 1:
Das Unternehmen nutzt das Microsoft-Portfolio aus Office, Sharepoint und Exchange. So liegt es nahe, hier auch die Einführung von OCS zu prüfen. Die vorhandene TK-Anlage würde erhalten bleiben und zu Beginn weiterhin die meisten Arbeitsplätze abdecken. Mit Microsoft OCS würde Unified Communications schrittweise eingeführt und gezielt an die Arbeitsplätze gebracht, die davon profitieren.

Alternative 2:
Das Unternehmen folgt dem Migrationsweg der traditionellen Anbieter und führt seine TK-Lösung schrittweise über die nächsten Jahre in deren Unified Communications Welt über. Die Microsoft-Welt wird über vom Hersteller bereitgestellte Schnittstellen integriert.

Alternative 3:
Das Unternehmen sieht keinen Sinn in einer langfristigen Migration und bevorzugt die sofortige Komplettumstellung. Der zum Teil auch teure Parallelbetrieb zweier Systeme wird vermieden. Zwar fallen einmalig erhebliche Migrationskosten an, aber auf Dauer werden Kosten und Arbeiten gespart. Diese Alternative geht nicht mit Microsoft.

Grundannahme aller drei Alternativen ist, dass jedes Unternehmen in den nächsten Jahren auf eine SIP-basierte Unified Communications-Lösung umstellen wird. Die Frage ist nicht ob, sondern wann und wie.

Die Frage, welcher Weg der für ein Unternehmen beste ist, hängt eng mit der Beantwortung einiger zentraler Fragen zusammen. Das ComConsult OCS-Forum 2009 analysiert diese Fragen und stellt die Ergebnisse exklusiver Test- und Projektarbeiten vor:



Wir stellen unsere exklusive Analyse der Microsoft-Strategie auf dem Forum vor. Was kommt in den nächsten Jahren und in welchem Umfang können damit auch weitergehende TK-Anforderungen abgedeckt werden?

2. Wohin geht die Kommunikationswelt in den nächsten Jahren? Wie viele Arbeitsplätze brauchen Unified Communications wirklich? Wie zwingend ist der Weg in Kollaborations-Lösungen? Welche Rolle werden Standards wie SIP spielen?

3. Wie zwingend ist der Zusammengang zwischen Office, Sharepoint, Exchange und OCS wirklich? Hat man als Microsoft-Kunde Nachteile, wenn man nicht OCS einsetzt, sondern auf die Produkte der TK- und Netzwerk-Anbieter setzt?

4. Wie einfach oder aufwendig ist der Parallelbetrieb zweier Systeme in der Form OCS und klassisches TK-System? Wie überzeugend ist die Kopplung aus OCS und TK-Anlage? Was muss die Schnittstelle leisten, welche Funktionalität geht verloren, skaliert das überhaupt?

5. Wo steht Microsoft mit dem OCS technisch? Sind die neuen Codecs für Sprache und Video wirklich besser? Wie überzeugend ist die neue Video-Strategie mit der Integration von HD-Video in den Desktop? Wie ist die Integration in die Kollaborations-Plattform Sharepoint zu bewerten?

6. Was leisten die Alternativ-Lösungen von Avaya, Alcatel, Cisco, Nortel, Siemens und Co? Hat es Vorteile, auf eine Unified Communications Lösung aus einer Hand zu setzen? Wo kommt dann der Kollaborations-Teil her?

7. Wie wichtig wird die Architektur der Lösung? Avaya und Siemens gehen mit neuen Produkten konsequent in Richtung virtualisierter SOA-Lösungen. Technisch spricht sehr viel für diese neue Art von Architektur. In welchem Umfang ist die Architektur der Lösung wichtig für die Produkt-Entscheidung?

8. Was leisten die Integrations-Pakete der verschiedenen Hersteller in die Microsoft-Welt? Wo liegen technische Unterschiede? Alles Marketing oder sind angebotenen Schnittstellen eine echte Alternative?

9. Wie teuer sind OCS und die Alternativen wirklich? Der Einstieg in OCS kann für große Microsoft-Kunden sehr preiswert erfolgen. Wie hoch werden die Kosten mittel- und langfristig, wenn immer mehr Arbeitsplätze erschlossen werden? Wie sieht die Wirtschaftlichkeit im Vergleich zu den anderen Lösungen aus?

10. Was macht der Wettbewerb? Die Rolle der klassischen TK-Anbieter wurde in den anderen Fragen schon angesprochen. Aber wo stehen speziell Cisco und IBM?

Das ComConsult OCS-Forum 2009 stellt exklusive Analysen vor, die elementare Hilfestellung zur Erarbeitung Ihrer TK-/Video- und Kollaborations-Strategie geben. Unter der Leitung der Top-Experten Dr. Jürgen Suppan und Dr. Frank Imhoff untersuchen wir die vorgestellten Fragen, geben Empfehlungen und berichten über aktuelle Erfahrungen. Ausgesuchte Hersteller stellen sich der Diskussion und zeigen ihre Antworten zu den Fragen auf.

Diese Veranstaltung ist ein absolutes Muss für Jeden, der sich mit Sprach-, Video, Multimedia- und Kollaborations-Lösungen befasst. Versäumen Sie nicht, sich rechtzeitig einen Platz in dieser herausragenden Ver-

Neuer Kongress

ComConsult Verkabelungs- und Infrastrukturforum 2009

Die ComConsult Akademie veranstaltet vom 27.04 - 28.04.09 ihren Kongress „ComConsult Verkabelungs- und Infrastrukturforum 2009“ in Bonn.

Verkabelungsprojekte werden aktuell mit einer Reihe komplexer Fragen konfrontiert, die insbesondere dadurch erschwert werden, dass eine anwendungsneutrale Kommunikationsverkabelung in der Regel auf 10 Jahre Nutzungsdauer ausgelegt wird:

1) Twisted Pair Fragen
- Mit welchen Datenraten ist in den nächsten 10 Jahren an welchen Stellen zu rechnen?
- Kat 6a kontra Kat 7a, was ist das richtige Kabel? Welchen Mehrwert bringt die im Vergleich deutlich teurere 7a-Verkabelung?
- Wie ist mit bestehenden Kat 5 und Kat 6 Verkabelungen umzugehen, müssen diese ersetzt werden oder gibt es wirtschaftliche „Aufrüst“-Lösungen?
- Welchem Stecker gehört die Zukunft? Wohin tendieren die Komponenten-Hersteller?
- Wie ist mit Kabel-Sharing umzugehen, hat das noch eine Zukunft?
- IP-Telefonie und Datenverkabelung: separat oder integriert? Was ist die wirtschaftlich und technisch optimale Anschlussdichte?
- Wo stehen die „Verkabelungsnormen“ heute, warum verzögert sich die seit langem erwartete Revision der EN 50173?

2) Glasfaser-Fragen
- Mit welchen Datenraten ist in den nächsten 10 Jahren an welchen Stellen zu rechnen, ist bei 40 oder 100 Gigabit ein sinnvolles Maximum erreicht?
- Welche Faser ist für welche Entfernung und welche Datenrate optimal?
- Hat sich die OM3-Faser im Multimode-Bereich durchgesetzt und wie können mögliche Vorteile genutzt werden?
- Müssen Nutzer von OM2-fasern mit Nachteilen rechnen? Was ist hier zu tun?
- Sollte überhaupt noch Multimode verlegt werden oder ist nun endlich die Zeit der reinen Single Mode-Verkabelung gekommen?
- Brauchen wir einen neuen Glasfasersteckertyp? Welche Stecker werden diskutiert? Wo liegen Vor- und Nachteile? Was machen die Komponenten-Hersteller, die dieses Rennen letztendlich entscheiden?
- Lassen sich Umgebungen mit gemischten LWL-Steckertypen überhaupt vermeiden, wie ist damit umzugehen?

3) Spezialthema: Rechenzentrumsverkabelung
- Welche Bandbreiten werden hier gefordert?
- Wird überhaupt eine spezielle Verkabelung gefordert oder reicht die bestehende Technik der Arbeitsplatzverkabelung aus?
- Welche Kabel- und Steckertechnik wird durch die Server- und Speicher-Hersteller bevorzugt werden?
- Wie ist mit den extrem hohen Packungsdichten umzugehen?
- Was machen die Switch-Hersteller, wie sieht das zukünftige Aktiv-Szenario für das Rechenzentrum aus?
- Wie lässt sich die Energieeffizienz in einem Rechenzentrum verbessern?
- Welche Rolle spielt die Sicherheit der Energieversorgung in einem Rechenzentrum?

4) Praxiserfahrungen bei Installation und Betrieb von Kommunikationsverkabelungen
- Welche Elemente einer Verkabelung müssen in welcher Form dokumentiert werden?
- Welche Werkzeuge stehen zur Verwaltung von Verkabelungen zur Verfügung, gibt es „die automatische Dokumentationsverwaltung“?
- Was ist die Grundlage für eine normgerechte Einmessung einer kupferbasierenden 10 Gbit/s-Verkabelung?
- Wie ist der Stand der Normung für Twisted-Pair-Messungen?
- Welche typische Installationssünden sind zu kennen und zu vermeiden?

An diesen Fragen setzt unser hochaktuelles Verkabelungs- und Infrastrukturforum 2009 an. Top-Verkabelungsexperten informieren Sie über die neuesten Entwicklungen. Referenten mit vollkommen unterschiedlichen Technologie-Strategien stellen sich der Diskussion mit dem Publikum und ihren Mitrednern. Neben kontrovers diskutierter Theorie bestimmt die „erlebte“ Praxis einen wesentlichen Anteil der Inhalte, die Veranstaltung ist damit ein absolutes Muss für jeden praxisnahen Verkabelungsplaner.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Verkabelungs- und Infrastrukturforum 2009

Ich buche den Kongress

☐ **ComConsult Verkabelungs- und Infrastrukturforum 2009**
27.04. - 28.04.09 in Bonn
zum Preis von € 1.690,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich ein Hotelzimmer

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

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

Programmübersicht Verkabelungs- und Infrastrukturforum 2009

Montag, den 27.04.2009

9:30 - 11:00 Uhr

Stand und Trends der informationstechnischen Standortverkabelung

- Internationale und europäische Normen ISO/IEC 11801 und EN 50173
- Anwendungsbereiche (50173-2 bis -X)
- Übertragungs- und Installationsstrecken: Klassen EA , FA und optische Klassen
- Modellierung
- Komponenten: Kategorien 6A , 7A , OM4
- Installation EN 50174-X
- Ausblick

Prof. Dr. Albrecht Oehler, Hochschule Reutlingen

11:30 - 12:15 Uhr

Installation strukturierter Verkabelung - Theorie und Praxis - zwei Welten treffen aufeinander

- Anforderungen der Normen und praktische Umsetzung
- Wie sieht die Installations"-pflicht" aus, wie die „-kür"?
- Gutes von Schlechtem unterscheiden
- Typische Installationsfehler (Wichtig! Fortlaufende Bauaufsicht)
- Fehler bei der Abnahme erkennen

Mark Groten, ComConsult Beratung und Planung GmbH

12:15 - 13:00 Uhr

Energieeffizienz im RZ: Schränke, Strom, Kühlung

- Immer mehr Server und Komponenten auf immer weniger Raum
- Wie sollten Schränke angeordnet sein?
- Wie lassen sich Stromverbrauch und Klimaleistung minimieren?
- Was ist bei Auswahl und Dimensionierung einer USV zu beachten?
- Wie lässt sich der Energiebedarf der Infrastruktur überwachen?

Matthias Egerland, ComConsult Beratung und Planung GmbH

14:30 - 15:15 Uhr

Verkabelungsstrategien ab 2009: zwischen Terabit Ethernet und Gigabit Wireless

- 10/40/100 Gigabit Ethernet
- Impulse aus der Optischen Übertragungstechnik und die Konsequenzen für MMF und SMF
- Generisches Optisches Transceiverdesign bis Terabit Ethernet
- 40 GBASE-T
- Multigigabit Wireless: Umwälzungen im Tertiärbereich

Dr. Franz-Joachim Kauffels, Unternehmer

15:15 - 16:00 Uhr

Die korrekte Feldmessung von installierten Klasse E_A und F_A Systemen

- Grundlagen für die Interoperabilität (Mix & Match) und die Bedeutung des Teststeckers
- Stand der Normierung von Klasse E_A aus dem Blickwinkel der Feldmessung
- Normative Richtlinien zur Feldmessung: ISO/IEC 61935-1
- Integration/Export der Messergebnisse in externe Systeme (z.B.: Asset Management)

Christoph Schillab, FLUKE Europe B.V.

16:30 - 18:00 Uhr

Sanierung bestehender RZ-Verkabelungen

- Neue Verkabelung gefordert
- Kabel-Standards
- Reduzierung der Kabelmenge
- Architekturen
- Kabeltypen: Twisted Pair, Fibre Optic, welche Faserqualität?
- Stecker und Aufbau von Rangiersystemen

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

11:00 - 11:30 Uhr Kaffeepause
13:00 - 14:30 Uhr Mittagspause
16:00 - 16:30 Uhr Kaffeepause
ab 18:00 Uhr Happy Hour

Dienstag, den 28.04.2009

9:00 - 10:30 Uhr

Elektrische Sicherheit beim Redesign von RZ-Infrastrukturen

- Renovierung bestehender Kabel- und Stromsysteme
- Leitlinien für eine sichere Installation
- Gesetzliche Auflagen Neue Auflagen der VDE und des VDS Neue Unterverteilungen für Rechnerräume
- Vorgehensweise

Dipl.-Ing. Karl-Heinz Otto, Sachverständigenbüro Otto

11:00 - 11:45 Uhr

Cat.6_A versus Cat.7_A

Bei dem 10Gbit Ethernet setzen die Aktivhersteller weiter auf den RJ45. Durch die aktive Kompensation der Störgrößen in den Signalprozessoren der Eingangsbaugruppen stellt sich die Frage nach dem Nutzen der Cat.7_A Stecksysteme.

- Wie groß sind die Performance Vorteile gegenüber Cat.6_A Stecksystemen?
- Welchen Weg geht die IEEE bei der Normierung des 100GBit Ethernets?
- Gibt es einen Trend zu einem einheitlichen Cat.7_A Steckgesicht?
- Wie sieht aus heutiger Sicht eine zukunftsweisende Verkabelung aus?

Stefan Ries, Reichle & De-Massari GmbH

11:45 - 12:45 Uhr

Nutzbarkeit von modernen Kommunikationsverkabelung für Meldeanlagen und Industrie

- Eine Verkabelung für alles?
- Nutzbare und nichtnutzbare Teilelemente der EN 50173-1
- Vor- und Nachteile der Klasse D, E und F und Glasfaser
- Produktsituation

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

10:30 - 11:00 Uhr Kaffeepause
12:45 - 14:00 Uhr Mittagspause
Ende der Veranstaltung 16:00 Uhr

14:00 - 15:00 Uhr

IP-basierte Videoüberwachungstechnik

- Digitale Videoüberwachung im Vergleich zu analoger und hybrider Technik
- Warum erfordert die Planung einer IP-basierenden Videoüberwachung einen anderen Technologieansatz als herkömmliche Videoübertragung?
- Maßnahmen zur Vorbereitung eines Lokalen Netzes bei Einführung von Videoüberwachung
- Bedeutung von Übertragungsrate, Verfügbarkeit, Delay, Jitter
- Sinn und Nutzen ereignisgesteuerter Überwachung und die Bedeutung von Bildbegleitinformationen

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

15:00 - 15:30 Uhr

Wo lohnt sich der Einsatz von Verkabelungsdokumentation?

- Einsatzszenarien
  - RZ-Räume, Equipment-Räume
  - Compliance und Audits
  - Komplexität und Dichte gegen Bereitstellungszeit und Qualität
- Erfassung von Verkabelungsstrukturen
- Change Management

Heiko Soldan, AixpertSoft GmbH

15:30 - 16:00 Uhr

Bessere Quality of Service durch Intelligentes Infrastruktur Management

- Was ist Intelligentes Infrastruktur Management (nach ITIL)?
- Wo wird Infrastruktur Management positioniert?
- Warum muss die Infrastruktur verwaltet werden?
- Traditionelle Dokumentations-, Management- und Planungstools
- Normen und Gesetze
- Basisfunktionen eines Infrastruktur Management Systems am Beispiel AMPTRAC
- Systemkomponenten und Software Eigenschaften
- AMPTRAC Hardware- Funktionsprinzip
- Vorteile eines intelligenten Infrastruktur Management Systems

Dipl.-Ing. Jürgen Distler, Tyco Electronics AMP GmbH

ComConsult IT-Sicherheits-Forum 2009

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

IT-Architekturen sind im Wandel. Damit verbunden sind erhebliche neue Anforderungen an Sicherheitslösungen. Im Kern konzentrieren sich dabei die neuen Entwicklungen auf vier Bereiche:

- Virtualisierung im Rechenzentrum
- Mobile Mitarbeiter und Kollaborations-Anwendungen
- Neue Applikations-Architekturen auf dem Desktop
- Neue Netzwerk-Technologien

Virtualisierung im Rechenzentrum schafft einen völlig neuen Bereich der Unsicherheit. Dies ist die Kommunikation der virtuellen Maschinen untereinander über den Hypervisor. Verbunden mit der Möglichkeit der automatischen Wanderung virtueller Maschinen auf andere physikalische Server entsteht die Frage, wie diese Kommunikation kontrolliert und gesteuert werden kann. Der Hypervisor-interne Softswitch muss als eigene Kommunikations-Instanz außerhalb des physikalischen Netzwerks gesehen werden. Hier stellt sich insbesondere die Frage, wie verhindert werden kann, dass bei der Verlagerung von virtuellen Maschinen die VLAN-Zugehörigkeit oder QoS verloren gehen.

Immer mehr mobile Mitarbeiter stehen vor der Herausforderung, an ihrem mobilen Arbeitsplatz unter voller Funktionalität arbeiten zu können. Dies beinhaltet auf der einen Seite wichtige Dienste wie Email und Kalender, aber auf der anderen Seite auch den Zugang zu Unternehmensapplikationen. Kombiniert man das mit den neuen Möglichkeiten der Desktop- und Applikations-Virtualisierung, dann wird deutlich, wie hoch der Bedarf der Anpassung der Sicherheits-Lösungen an diesen Bereich ist.

Neue Applikations-Architekturen auf dem Desktop binden den Desktop mehr und mehr in multimediale zentrale Dienste ein. Auf der Basis von AJAX und anderen Web 2.0-Hilfsmitteln werden leistungsstarke neue Applikationen geschaffen. Diese neue Applikationswelt schafft naturgemäß neue Risiken, die im Sicherheits-Konzept berücksichtigt werden müssen.

Das ComConsult Sicherheits-Forum 2009 stellt sich den aktuellen Herausforderungen der Sicherheitstechnik. Die neuesten Entwicklungen werden analysiert und bewertet. Die Referenten sind Topexperten aus dem Sicherheitsbereich, die Informationen sind eine Mischung aus aktuellen Projekterfahrungen, der Mitarbeit beim BSI und den Ergebnissen des ComConsult Research Labors.

Versäumen Sie nicht, sich rechtzeitig einen Platz in dieser herausragenden Veranstaltung zu sichern.

Frühbucherrabatt bis 30.04.09

ComConsult IT-Sicherheits-Forum
22.06. - 25.06.09 in Königswinter

Für Besucher unserer bisherigen Kongresse bzw. für die Teilnehmer am VIP-Verteiler bieten wir Ihnen exklusiv eine Vorbuchungsphase für das ComConsult IT-Sicherheits-Forum 2009 bis zum 30.04.2009 für eine rabattierte Teilnahmegebühr an.

ComConsult IT-Sicherheits-Forum 2009 zum Preis bei Buchung bis 30.04.09 von € 2.090,- statt regulär € 2.290,- zzg. MwSt.

Die Buchung innerhalb der Frühbucherphase ist verbindlich, kann aber jederzeit auf einen anderen Mitarbeiter Ihres Unternehmens übertragen werden.

Programmübersicht ComConsult IT-Sicherheits-Forum 2009

Montag, 22.06.09

9:30 Uhr - 11:00 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

11:30 Uhr - 12:30 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 Sicherheitskomponenten 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

14:00 Uhr - 16:30 Uhr
Sicherheit der Virtualisierungslösungen im Vergleich
Referenten von den Herstellern von Virtualisierungslösungen mit anschließender Podiumsdiskussion

16:30 Uhr - 17:15 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

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

Dienstag, 23.06.09

9:00 Uhr - 09:45 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

9:45 Uhr - 10:30 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

11:00 Uhr - 11:45 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

11:45 Uhr - 12:30 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

14:00 Uhr - 15:00 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

15:30 Uhr - 16:15 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

16:15 - 17:00 Uhr
Sicherheit in drahtlosen Kommunikationssystemen
- Überblick über gängige SAN-Technologien: Fibre Channel und iSCSI
- Sicherheitsprobleme: Zoning, Authentisierung, TCP-IP-Schwächen, Man-in-the-Middle-Angriffe
- Technische Schutzmaßnahmen
- Empfehlungen für sicheres SAN-Management

Dr. Joachim Wetzlar,
ComConsult Beratung und Planung GmbH

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

Mittwoch, 24.06.09

9:00 Uhr - 10:00 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

10:00 Uhr - 10:45 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

11:15 Uhr - 12:15 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

13:30 Uhr - 14:15 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

14:15 Uhr - 15:00 Uhr
Sicherheitsaspekte Dienst-orientierter Architekturen
- Von SOA über SaaS bis Cloud Computing: Konkurrierende 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

15:30 Uhr - 16:15 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 GmbH

16:15 Uhr - 17:00 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

Andreas Meder,
ComConsult Beratung und Planung GmbH

10:45 - 11:15 Uhr Kaffeepause
12:15 - 13:30 Uhr Mittagspause
15:00 - 15:30 Uhr Kaffeepause

Der Veranstalter behält sich Änderungen im Programm vor!

Programmübersicht ComConsult IT-Sicherheits-Forum 2009

Donnerstag, den 25.06.09 - Praxis-Workshops - Bitte kreuzen Sie 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 werden?

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

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
IT-Sicherheits-Forum 2009

Ich buche den Kongress
☐ **ComConsult IT-Sicherheits-Forum 2009**
22.06. - 25.06.09 in Königswinter
zum Preis von € 2.090,-* zzgl. MwSt.

Workshopauswahl

vormittag	nachmittag
☐ 1	☐ 1a
☐ 2	☐ 2a
☐ 3	☐ 3a

* gültig bis 30.04.2009 - dann regulär € 2.290,- zzgl. MwSt.

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

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

Zweitthema

IT-Verkabelung im Rechenzentrum: Beginn einer neuen Epoche?

Fortsetzung von Seite 1

Dipl.-Ing. Hartmut Kell kann bis heute auf eine mehr als 20-jährige Berufserfahrung in dem Bereich der Datenkommunikation bei lokalen Netzen verweisen. Als Leiter des Competence Center IT-Infrastrukturen der ComConsult Beratung und Planung GmbH hat er umfangreiche Praxiserfahrungen bei der Planung, Projektüberwachung, Qualitätssicherung und Einmessung von Netzwerken gesammelt und vermittelt sein Fachwissen in Form von Publikationen und Seminaren.

Definition und Spezifikation der zu betrachtenden Teilelemente

Jeder vernünftigen Planung von technischen Maßnahmen muss eine Analyse der Anforderungen vorausgehen. Dazu sind im ersten Schritt die Elemente zu kennen bzw. zu benennen, die dieser Anforderungsanalyse unterzogen werden müssen. Natürlich ist klar, dass es um Elemente einer Verkabelung geht, die es erlauben, einen Server an einen LAN-Anschluss anzuschließen. Viele ältere Rechenzentrumsumgebungen nutzen dazu Anschlussschnüre, die direkt zwischen dem Server und dem aktiven Koppelement, meistens ein Switch, „geschaltet“ werden. Das hätte zur Folge, dass in einem Rechenzentrum lediglich ein einziges Verkabelungselement notwendig wäre. (siehe Abbildung 1)

Doch gerade das häufig dokumentierte Kabelchaos entstand genau durch diese Methodik: Je nach Bedarf wurden Anschlussschnüre mit unterschiedlichen Medien (Kupfer oder LWL) und unterschiedlichen Längen verwendet und zwischen den beiden Anschlusspunkten verlegt. Dabei bestand die Verlegung aus einem einfachen Einziehen der Kabel in die vorhandenen Kabelführungssysteme, welche zumeist lediglich durch

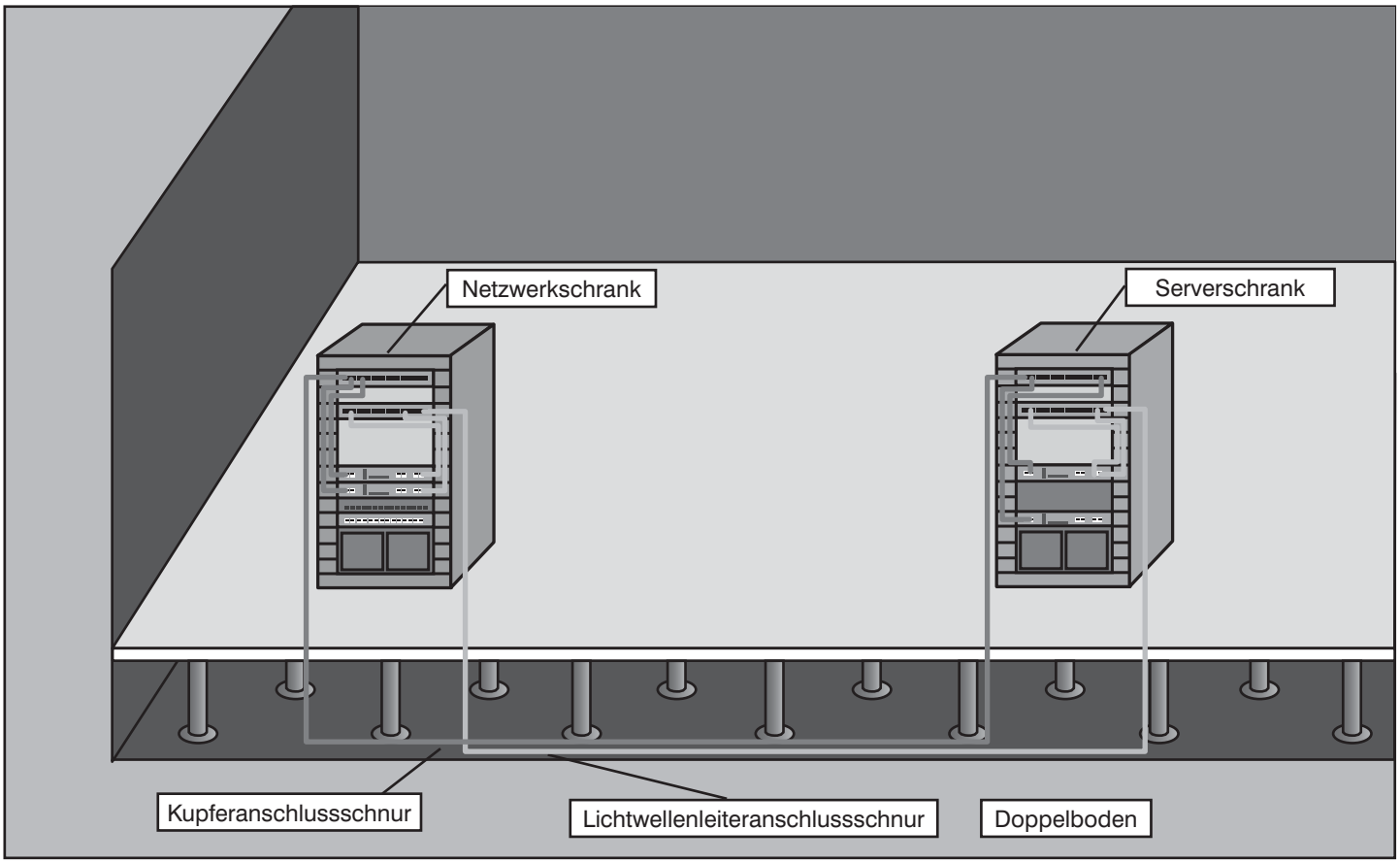


Abbildung 1: RZ-Verkabelung der einfachen Art

einen Doppelboden repräsentiert wurden. Es wurden keinerlei Regeln der „Normal-Installation“ beachtet, viel mehr orientierte man sich an dem „provisorischen“ Charakter der Verkabelung von der Dose bis zum Endgerät. Damit verbunden unterblieb auch jede Art der Dokumentation (alles sollte ja nur provisorisch sein) und das Chaos wurde mehr und mehr. Die unangenehmen Seiten dieser Methodik fallen erst dann auf, wenn z.B. Erweiterungsplanungen größeren Ausmaßes anstehen wie Komplett-Umzüge von ganzen Server-Racks. Auch Ausfälle der Verkabelungsinfrastruktur im Rechenzentrum, die aufgrund des nicht dokumentierten Chaos nur sehr schleppend behoben werden können, machen deutlich, dass diese Verfahrensweise ungeeignet ist für sehr große Rechenzentren, aber bereits in kleineren Serverräumen mit dem Anspruch der hohen Verfügbarkeit stellt sie ein Risiko dar. Alternativen müssen her und nach dem Prinzip „das Rad nicht neu erfinden“ ist zu überlegen, welche Techniken sich bewährt haben. Unter Berücksichtigung weniger verbleibender Unzulänglichkeiten darf rückblickend gesagt werden, der Ansatz der strukturierten Kommunikationsverkabelung nach der EN 50173 (bzw. ISO/IEC 11801 oder EIA/TIA 568) war erfolgreich. Dieser Ansatz der Normierung hat es geschafft, eine Verkabelungsinfrastruktur einzuführen, die in Abhängigkeit der Bedürfnisse unterschiedlich skalierbar ist und vielfältige Qualitätsklassen zulässt. Erst durch Standardspezifikationen innerhalb dieser Normen wurde dem Planer bzw. Nutzer eine Stabilität und Sicherheit gewährleistet, welche zu der hohen Nutzungsdauer der aktuellen Verkabelungen geführt hat. Dabei besteht das Erfolgsgeheimnis der Standards einfach ausgedrückt aus zwei Prinzipien, der Spezifikation von Verkabelungsteilelementen und der Empfehlung (nicht Vorschrift!) zur Verknüpfung der Teilelemente in bestimmten Topologievarianten. Der Autor geht davon aus, dass allen Leser die 3-stufige, in Primär-, Sekundär- und Tertiärbereich unterteilte Topologie bestehend aus den Elementen Standortverteiler, Gebäudeverteiler, Etagenverteiler, Sammelpunkt (optional) und Teilnehmeranschluss bekannt ist. Eine wesentliche Stärke der favorisierten sternförmigen Topologie resultiert aus der Skalierbarkeit, jede Ebene der Hierarchie kann durch Verwendung von unterschiedlichen Materialien unabhängig von den anderen Ebenen skaliert werden. Überträgt man diesen Ansatz auf die Verkabelung eines Rechenzentrums, so lässt sich auch hier dieser Vorteil nutzen. Dazu wäre es notwendig, dass Rechenzentrum in verschiedene Bereiche einzuteilen. Der Ansatz der aktuellen, für die Rechenzentrumsverkabelung „zuständigen“ europäischen Norm EN 50173-5 sieht dies vor, dabei wird diese Rechenzentrumsverkabelung nicht in die bisherige Struktur der EN 50173-1 integriert, was einen Neuaufbau der Norm zur Folge hätte, sondern sie wird als Ergänzungsmodul definiert. Diese Ergänzung unterscheidet sich zur EN 50173-1 in erster Linie durch die Definition von neuen Teilelementen in der Topologie (Definition von neuen Verteilernamen, neuen Bezeichnungen der Verkabelungen zwischen diesen Verteilern). Die übertragungstechnischen Anforderungen an die Datenverkabelung sind (mit Ausnahme der Glasfaserverkabelung) im Wesentlichen identisch zur EN 50173-1. Es ist weitestgehend eine Übernahme der dort erläuterten Spezifikationen möglich, Abweichungen werden im Verlauf des Artikels noch beschrieben. Abbildung 2 zeigt diese neuen Elemente und Bereiche.

- GA steht für Geräteanschluss und entspricht dem Teilnehmeranschluss der Standardnorm. Die mechanische Unterbringung bzw. Befestigung der GA wird nicht in der Norm spezifiziert.

- BV steht für Bereichsverteiler, er bildet den eigentlichen Verteiler für das Rechenzentrum und seine Reichweite ist auf 90 m begrenzt (analog zum Etagenverteiler). Große Rechenzentren werden bedingt durch diese Längeneinschränkung mehrere BV besitzen.

- HV steht für Hauptverteiler, er sorgt für die Anbindung des Rechenzentrums an die ENS und den „50173-1-Verteiler“ und natürlich die Verbindung der Bereichsverteiler.

- ENS steht für Externe Netzschnittstelle, die z.B. zu einem Provider genutzt wird, sie kann innerhalb oder außerhalb des Rechenzentrums liegen.

- LVP steht für Lokaler Verteilerpunkt (optional) und er bildet analog zum Sammelpunkt ein optionales Element. Analog zum SP enthält er nur passive Verbindungen und muss min. 15 m entfernt vom BV sein.

Wichtig, auch hier gehört die Anschlussschnur, welche den Server an das LAN-Koppelelement anschließt, nicht zum Spezifikationsumfang der Norm.

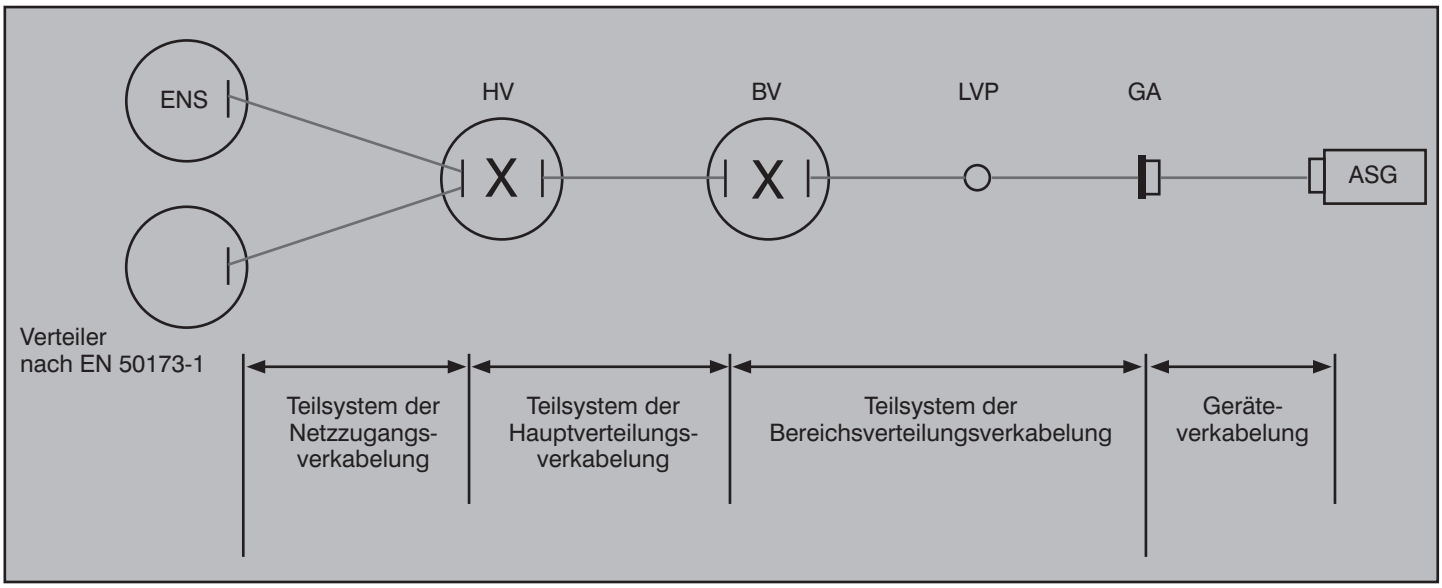


Abbildung 2: Teilsysteme eines Rechenzentrums nach EN 50173-5 (Quelle: EN 50173-5)

IT-Verkabelung im Rechenzentrum: Beginn einer neuen Epoche?

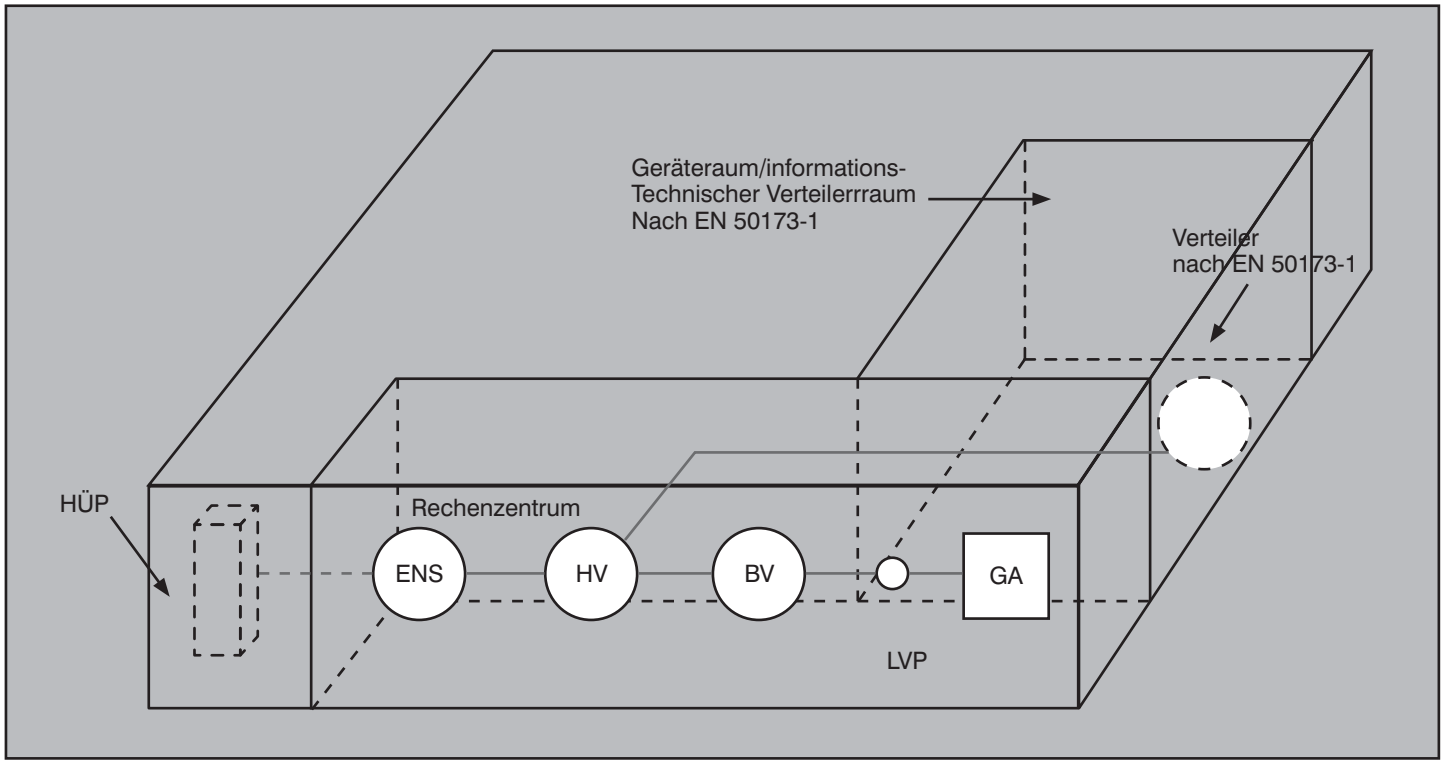


Abbildung 3: Räumliche Zuordnung der Teilelemente

Die räumliche Lage der neuen Verteiler beschreibt die EN 50173-5 durch Abbildung 3.

In der Praxis lässt sich dieses Prinzip wie folgt umsetzen: Im Rechenzentrum wird ein bzw. bei sehr hoher Anforderungen werden zwei oder mehr Netzwerkschränke vorgesehen, die neben der Verkabelung auch die aktiven Komponenten insbesondere Switches aufnehmen; diese Schränke nehmen keine Server auf. Dieser Schrank entspricht in der EN 50173-5 dem Typ „Bereichsverteiler“ BV. Von diesem Netzwerkschrank aus werden verschiedene Medien zu den Serverschränken SVS verlegt, dabei sind Installationskabel zu verwenden, keine Anschlussschnüre oder Rangierkabel, und beide Enden sind mit einer Buchse abzuschließen (bei Glasfaser entspricht dies in der Regel einer Kupplung). Sowohl im BV wie auch im Serverschrank sind die Kabelenden auf 19“-Rangierfelder aufzulegen. Vorhandene Serverregale, die keine Montage von 19“-Rangierfeldern zulassen, können statt dessen z.B. mit herkömmlichen Anschlussdosen ausgestattet werden. (siehe Abbildung 4)

Mit dieser Vorgehensweise werden u.a. folgende Verbesserungen erreicht:

- Bessere Auslegung und Positionierung der Verteiler, so dass Längen von Rangierschnüren und Geräteverbindungsschnüren minimiert werden und optionales Vorsehen von Redundanzen in der Verkabelung.
- Die Qualität der festverlegten und damit schlecht austauschbaren Kabelanteile ist wesentlich besser und damit zuverlässiger. Diese Kabeltypen erlauben auch bei größeren Längen eine höhere Übertragungsrate als flexible Anschlussschnüre.
- Der störanfällige Arbeitsbereich beschränkt sich auf den Rangierbereich im Netzwerkschrank und im Serverschrank, werden z.B. die dort verwendeten Schnüre beschädigt, muss kein

IT-Verkabelung im Rechenzentrum: Beginn einer neuen Epoche?

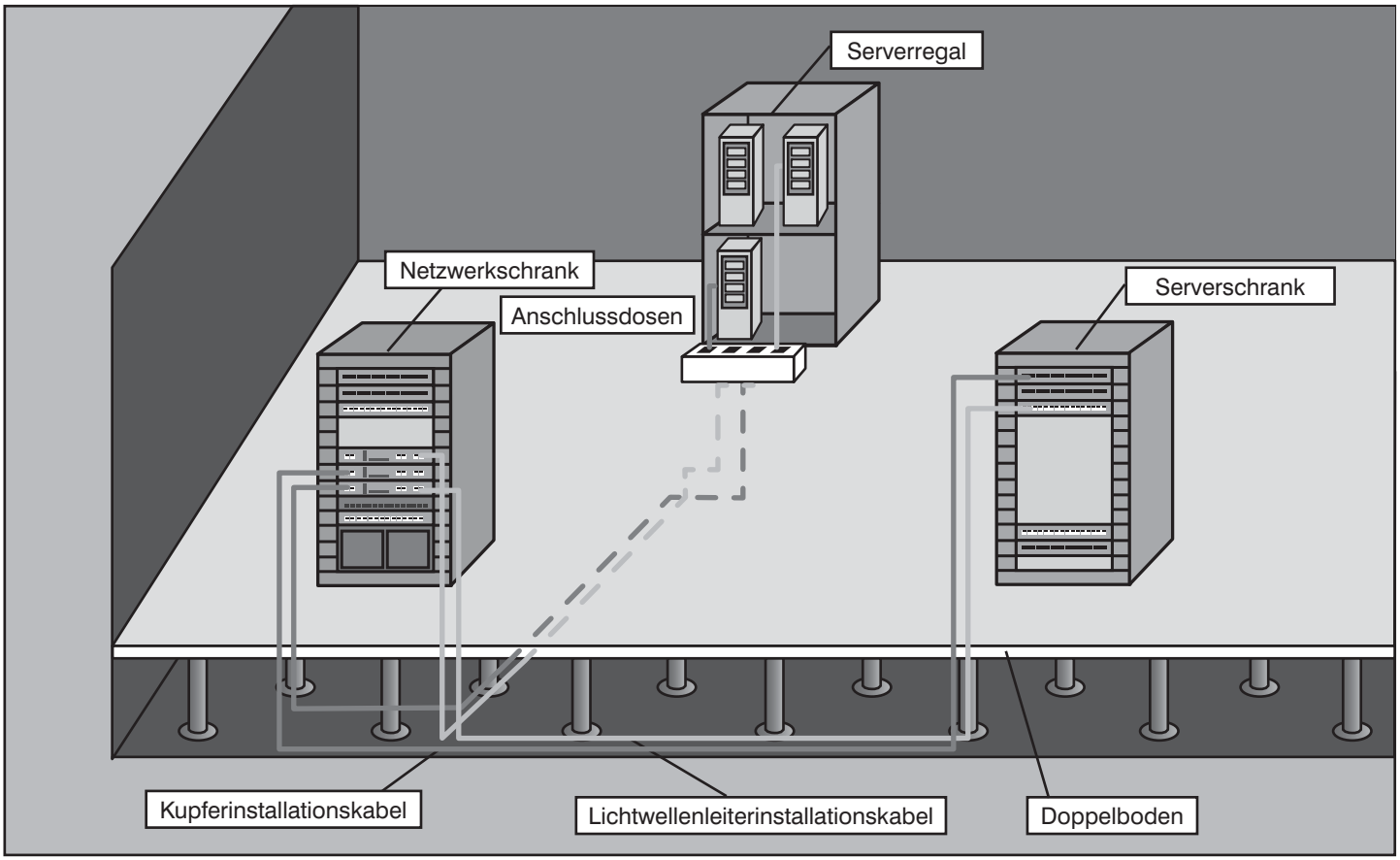


Abbildung 4: RZ-Verkabelung der modernen Art

Austausch der Kabel im Doppelboden vollzogen werden.

- Die Wahl des Anschlusssteckers im Kupfer-Rangierfeld sowohl des Netzwerkschrankes wie auch des Serverschrankes kann losgelöst von der üblichen Forderung nach RJ45-Kompatibilität getroffen werden. Mit Hilfe der Anschlussschnüre kann eine Adaption auf jede Anschlussbuchse der aktiven Netzwerkkomponenten wie auch der Server-Interfacekarten erfolgen. Eine ähnliche Freiheit bietet sich auch bei Glasfaser, hier ist der technisch beste Stecker in den Rangierfeldern vorzusehen.

- Die unzugänglichen Bereiche können dauerhaft dokumentiert und beschriftet werden.

Die Anordnung der Teilelemente innerhalb der Topologie sieht wie bisher eine sternförmige Hierarchie vor, Kennern der EN 50173-1 wird dieses Modell bekannt sein. Von vielen Planern wurde das entsprechend ähnliche Modell der EN 50173-1 als „die Topologie“ interpretiert und damit eine wesentliche Schwäche bei der Umsetzung mit eingebaut, der Single-Point-of-Failure der übergeordneten Verteiler. Im nachfolgenden Bild ist z.B. innerhalb des Rechenzentrums der HV ganz besonders auffallend, fällt dieser aus, ist die Kommunikation innerhalb des Rechenzentrums in weiten Bereichen unterbrochen. (siehe Abbildung 5)

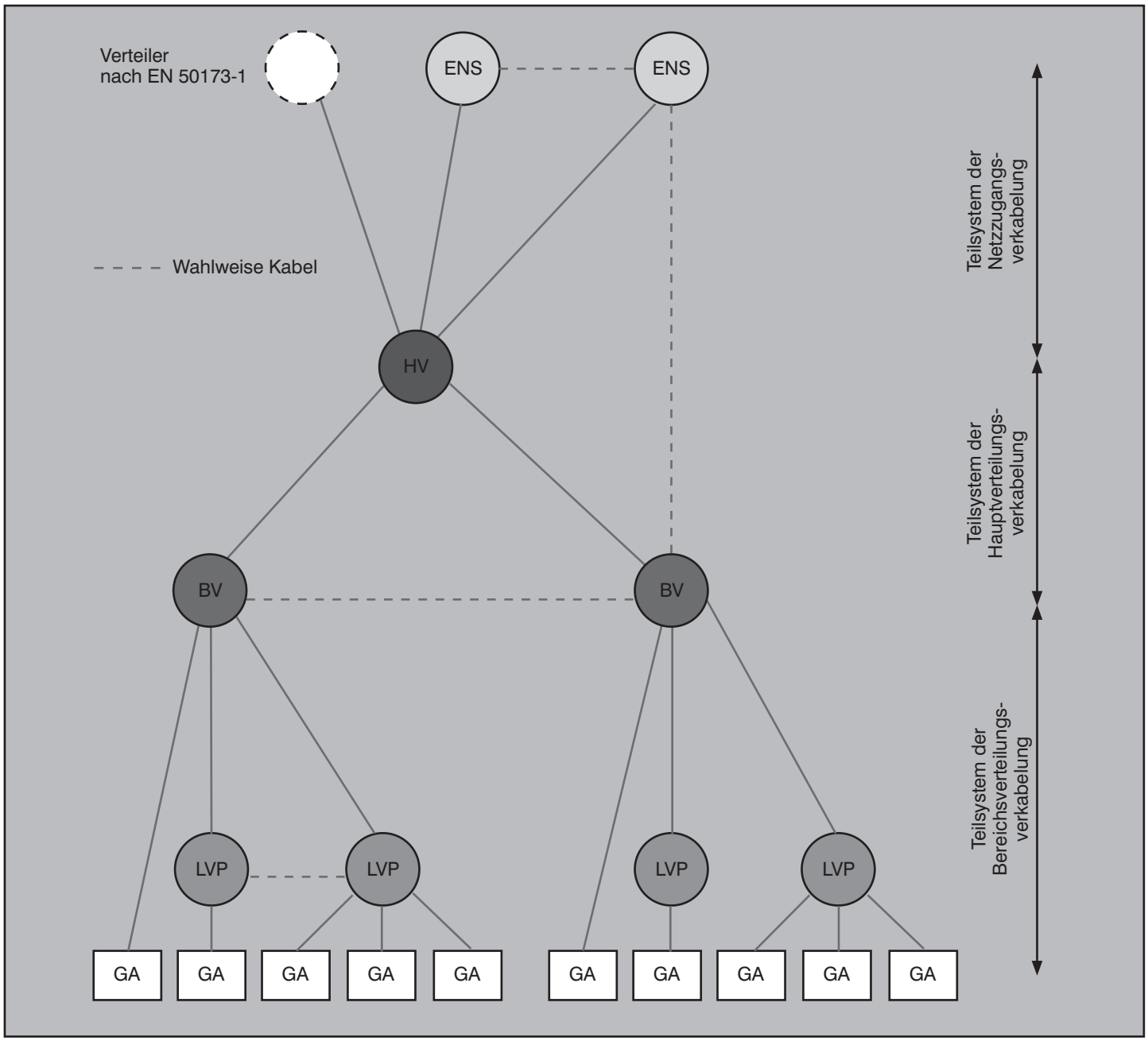


Abbildung 5: Niedrigverfügbare Topologie innerhalb des RZs

Im Unterschied zur EN 50173-1 wurde dieser Mangel jetzt bei der neueren Norm EN 50173-5 Dank eines weiteren hinzugefügten Bildes beseitigt, jedem Leser dieser Norm sollte damit klar werden, dass nur eine Vermeidung von Single-Point-of-Failure eine hohe Verfügbarkeit sicher stellen kann. (siehe Abbildung 6)

Auch IT-Verantwortliche, die keine großen Rechenzentren besitzen oder einzurichten haben, sollten sich des strukturierten Lösungsansatzes bemächtigen. Nachfolgendes Beispiel veranschaulicht dies, die oben beschriebenen Teilelemente sind auch hier ersichtlich. Es wurde ganz bewusst eine Trennung der Infrastrukturen für die Etagenverkabelung (Raum rechts) und des Serverraumes gewählt (in Analogie des Modulansatzes der EN). Gründe dafür lagen u.a. in der organisatorischen Trennung von Rechenzentrum und Netzwerkbetrieb. (siehe Abbildung 7)

Rechenzentrumsverkabelung mit Glasfaser

Nachdem oben die Gründe für die Einführung einer strukturierten Verkabelung in einem Rechenzentrum hergeleitet wurden, sollen nun nachfolgend die Anforderungen an die Materialien, insbesondere die nachrichtentechnischen Anforderungen, spezifiziert werden. Derzeit herrscht eine heftige Diskussion bereits bei der Frage, ob Glasfaser oder Kupfer das Medium der ersten Wahl im Rechenzentrum sein soll. Nach Meinung des Autors gibt es in diesem Punkt keine klare Empfehlung für einen der beiden Medientypen, das ist im Sinne einer strukturierten Verkabelung auch nicht zwingend notwendig. Aber es lohnt sich durchaus, die Vor- und Nachteile der beiden Techniken mit dem Hintergrund ihres Einsatzes im Rechenzentrum zu beleuchten.

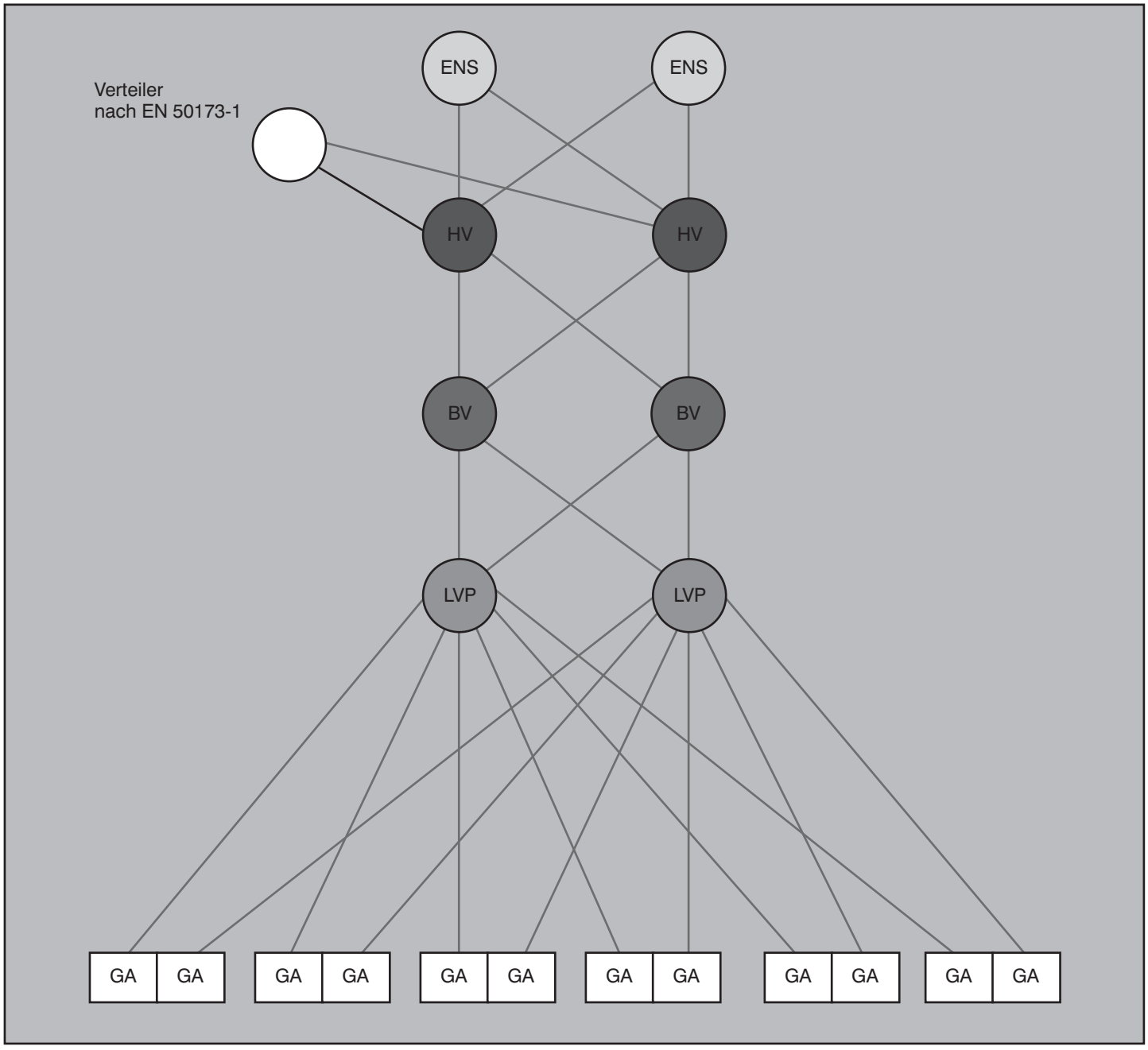


Abbildung 6: Hochverfügbare Topologie innerhalb des RZs

Die in Fachkreisen prognostizierte Steigerung der Datenrate (oftmals mit dem nicht ganz korrekten Begriff der Bandbreite umschrieben) wird nach aktuellem Stand der Technik am deutlichsten im Rechenzentrum sein, daran gibt es kaum Zweifel. Erfahrungen im Backbone-Bereich der meisten Netzwerke zeigen, dass eine Uplink-Datenrate von 1 Gbit/s derzeit für viele (noch) weit mehr als genügend ist, aber bereits eine Datenrate mit 1 Gbit/s mittel- und langfristig für Rechenzentren nicht mehr ausreichend sein wird. Galt seit vielen Jahren die Glasfaser als „das Medium“ mit der höchsten Bandbreite und damit „unbegrenzter“ Datenrate, so hätte sich dies (fast) als Irrtum erwiesen. Rechenzentrumsverkabelungen mit OM2 oder gar OM1-Faserqualität ließen bis 2006 für eine Datenrate mit 10 Gbit/s nach Standard nur eine Übertragungsreichweite von maximal 80 m (OM1 sogar nur etwas mehr als 30 m) zu, häufig selbst für ein Rechenzentrum zuwenig. Damit wäre die Übertragungsreichweite nicht besser als bei der aktuellen Kupfertechnologie 10GBaseT mit 100 m gewesen. Glücklicherweise wurden 2006 mit dem neuen Standard 10GBaseLRM auch für diese Medien Reichweiten bis 220 m ermöglicht. Berücksichtigt man eine Untersuchung, veröffentlicht durch die Firma Corning, so wird deutlich, dass 87% aller Links im Rechenzentrum kürzer als 150 m sind (95% kürzer als 200 m und fast 100% kürzer als 300 m). Damit ließe sich mit den angeführten Techniken nach aktuellem Stand fast jedes Rechenzentrum mit Hilfe eines einzigen Bereichsverteilers aufbauen, von dem aus jeder Server über Glasfaser erreicht werden könnte, selbst die „Schallmauer“ von 300 m könnte bei

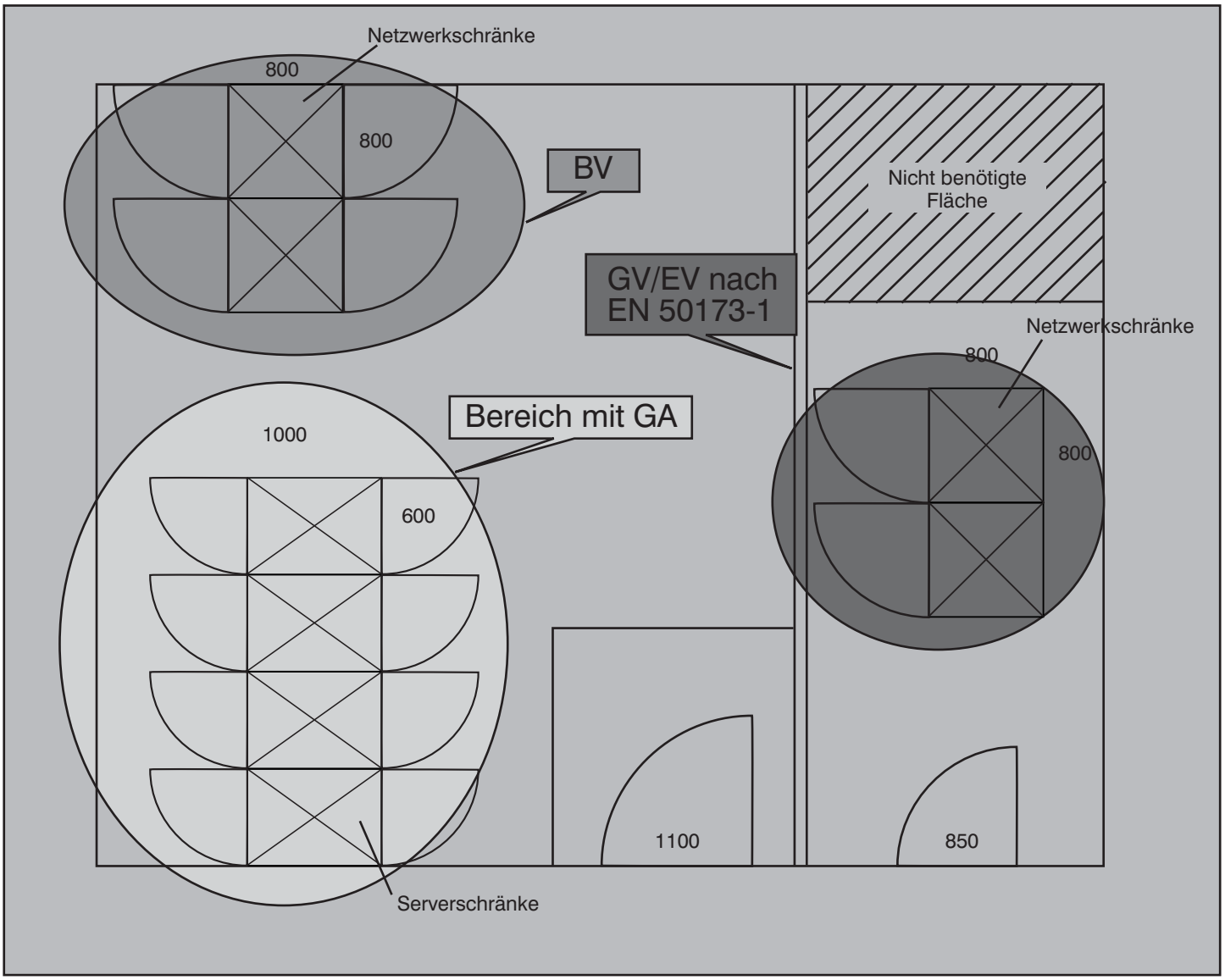


Abbildung 7: Beispiel eines kleineren Serverraumes

Einsatz von „verbesserten“ OM3-Fasern noch erheblich überschritten werden. Beispielsweise sichert Corning mit der Glasfaser Infinicor eSX+ eine Reichweite von 550 m für eine Datenrate von 10 Gbit/s zu. Aktuelle Diskussionen der Ethernet-Normierungsgremien machen deutlich, dass bei der nächsten Entwicklungsstufe 100 Gbit/s eine Weiterverwendung von OM1 und OM2 nicht zu erwarten ist, es wird verstärkt auf die bereits standardisierte OM3 oder die als Standard beabsichtigte OM4-Faser gesetzt. Zu beachten ist dabei, dass bei 40 Gbit/s oder 100 Gbit/s über Glasfaser zwar auch eine „normale“ OM3-Faser berücksichtigt werden wird, diese aber möglicherweise „nur“ bis 100 m verwendet werden kann (z.B. mit 100GBASE-SR10). Demzufolge ist Vorsicht walten zu lassen bei Aufbau einer zentralen Rechenzentrumsverkabelung in großen Rechenzentren, hier können langfristige Nachverkabelung auch bei Einsatz von OM3 (oder OM4) nicht ausgeschlossen werden. Tabelle 1 zeigt den Unterschied zwischen den 4 Faserarten. Im Übrigen spielen Singlemodefasern trotz der potenziell höheren Reichweiten innerhalb eines Rechenzentrums aufgrund der sehr hohen Kosten bei den aktiven Systemen so gut wie keine Rolle.

Folgt man also der Empfehlung, im Rechenzentrum keine Neuverlegung von OM1 und OM2 mehr vorzunehmen, stellt sich die Frage, wie es sich mit Verkabelungen verhält, bei denen bereits OM1 oder OM2 verwendet wurde, müssen diese entfernt werden? Das Problem des Mischens von Glasfasern ergibt sich natürlich nicht nur im Rechenzentrum, bei jeder „gewachsenen“ Glasfaserumgebung muss sich die Frage gestellt werden, ob ein irrtümliches Verschalten von alten und neuen Fasern zu Fehlern führen kann. Nach Aussage der Kabelhersteller gibt es zu diesem Punkt in den Fachkreisen geteilte Meinungen, es überwiegt die Einschätzung, dass auf kurzen Strecken, und damit ist ja bei falscher Verwendung von Anschlussschnüren zu rechnen, der Unterschied der unterschiedlichen Modendispersionen sich nicht negativ auswirken sollte. Bewahrheitet sich diese Einschätzung, so dürfen wohl auch bzw. gerade im Rechenzentrum ältere Fasern beibehalten werden, vor allem dann, wenn durch Verwendung von unterschiedlichen Steckern bzw. Kodierungen oder Farbmarkierungen an den Kupplungen Fehlschaltungen vermieden werden können.

IT-Verkabelung im Rechenzentrum: Beginn einer neuen Epoche?

Kategorie		OM1	OM2	OM3	OM4*
Kerndurchmesser	µm	50 und 62.5	50	50	50
Größte Dämpfung in db/km	850nm	3,5	3,5	3,5	
	1300 nm	1,5	1,5	1,5	
Mininmale Bandbreite bei Vollanregung (MHz*km)	850nm	200	500	1500	1500
	1300 nm	500	500	500	500
Minimale Laserbandbreite	850 nm	nicht spezifiert	nicht spezifiert	2000	4700

* noch kein Standard, deshalb Werte unter Vorbehalt

Tabelle 1: Multimode-Fasertypen nach Standard

Damit wären wir an einem weiteren Punkt, der zu spezifizieren ist; was ist der beste Glasfaserstecker? In diesem Punkt lässt uns die Norm weitestgehend alleine, die deutliche Fokussierung auf 1 bis 2 Systeme wie bei den kupferbasierenden Techniken findet man bei Glasfaser nicht. Schaut man die letzten 20 Jahre zurück, so hat sich gezeigt, dass fast keiner der gerade bei den aktiven Komponenten modernen Steckverbinder die gleiche Zeitlosigkeit besessen hat wie der RJ45 in der Kupferwelt. Vom ST angefangen über den SC bis hin zu den insbesondere bei den aktiven Komponenten anfänglich sehr beliebten MTRJ glaubten immer wieder viele Planer, auch die installierte feste Verkabelung mit dem aktuell angesagten Stecker auszustatten. Daraus folgt als erste Konsequenz, dass sich eine bunte Vielfalt sowohl bei den aktiven Komponenten aber auch bei den Rangierfeldern entwickelt, ohne dass man dem Problem der Verwendung von Adapterkabeln auch nur annähernd entgeht. Als zweite Konsequenz ergibt sich heute, dass man den zur Zeit gerade bei SFP-Modulen favorisierten LC-Steckverbinder eigentlich auch im Rangierfeld vorsehen müsste, der Wildwuchs wächst weiter. Es ist für den Autor nicht schlüssig nachvollziehbar, warum man bei einer festen Verkabelung nicht eine Entscheidung für ein „gutes“ System treffen kann und dieses, unabhängig von der aktuellen Mode beibehält, bis es dann tatsächlich ein neues System gibt mit deutlichen Vorteilen. Planungen, bei denen über viele Jahre hinweg bewährte Systeme wie z.B. der E2000 konsequent beibehalten und damit Wildwuchs verhindert werden konnte, vereinfachen den Betrieb.

Reichen die Überlegungen zu Auswahl der Glasfaser und des Steckers jetzt aus? Leider nein. Würde man von einem zentralen Bereichsverteiler einzelne niedrigfaserige Glasfaserkabel bis zu jedem Geräteanschlusspunkt verlegen, so wird man eine wesentliche Stärke des Mediums nicht nutzen. Die Stärke besteht darin, dass sich viele physikalische Übertragungskanäle sprich Fasern in einem einzigen – relativ dünnen – Kabelmantel störungsfrei „verpacken“ lassen. Dies bedeutet konkret, dass man mehrere Dutzend Fasern in ein Kabel packen kann, dieses Kabel bis zu gleichmäßig verteilten festen Aufteilpunkten führt und von hier aus dann mit niedrigfaserigen Kabeln zum Beispiel in die Serverracks geht und dort die Fasern auf Stecker bzw. Kupplungen auflegt. Dies hat den entscheidenden, mit Kupfer so nicht nutzbaren Vorteil, dass die Kabelmenge im Doppelboden deutlich reduziert wird. Der Aufteilpunkt kann als Spleißverteiler mit festen Spleißverbindungen ausgelegt werden oder aber auch als Lokaler Verteilerpunkt LVP mit Steckverbindungen. Ein LVP würde Änderungen bei Umpositionierungen von Serverracks oder auch Nachinstallationen vereinfachen, neue Kabel müssen nicht immer komplett bis zum zentralen Bereichsverteiler durch den gesamten Doppelboden verlegt werden. Neben selbst entwickelten Lösungen sind auch spezielle LVPs für die Montage an Stützen von Doppelböden auf dem Markt verfügbar, ein Beispiel bietet der Hersteller Rosenberger an.

Rechenzentrumsverkabelung mit Kupfer

Die übertragungstechnischen Kapazitäten von Multimodefasern (fast) jeden Typs erlauben ein Rechenzentrum mit zentral aufgebauter Datenverkabelung, eine Kupferlösung ausgehend von einem einzigen Bereichsverteiler dagegen wird ab einer Raumgröße von ca. 1600 m2 kaum gelingen. Doch genauso wenig wie bei einer Gebäudeverkabelung die Argumentation sinnvoll sein kann, nur eine zentrale Verkabelung mit „Glasfaser bis zum Arbeitsplatz“ sei eine richtige Verkabelung, so gibt es auch keine festgeschriebene Notwendigkeit zu einer zentralen Verkabelung im Rechenzentrum. Stattdessen erlaubt die Norm die Bildung von verschiedenen Bereichen mit unterschiedlichen Medien und unterschiedlichen Längenrestriktionen. Sollte das Rechenzentrum also eine größere Ausdehnung haben, wird man einen Hauptverteiler vorsehen müssen, der die angeschlossenen Bereichsverteiler dann wahlweise über Kupfer oder LWL anbindet, die vom Bereichsverteiler ausgehende Verkabelung ließe sich dann analog zum Etagenverteiler wieder in TP realisieren.

Im Unterschied zur Glasfaser, die bei Einsatz eines Mediums mit mindestens OM3-Qualität zweifelsohne geeignet sein wird

für höhere Datenraten als 10 Gbit/s (selbst bei „kleinen Längen“), war diese Eignung für Twisted Pair bisher noch nicht ganz klar erkennbar. Der Autor verzichtet an dieser Stelle auf eine Herleitung der nachrichtentechnischen Anforderungen und daraus abgeleiteten Materialoptionen (Verweis auf den Fachartikel von Dr. Kauffels aus dem Netzwerk-Insider vom Januar 2009), die grundsätzlichen Kernschlussfolgerungen werden nachfolgend beschrieben. Sollten sich die derzeitigen Prognosen als richtig erweisen, so wird in jedem Falle eine Twisted-Pair-Verkabelung mit einer Qualität der Kategorie-7 oder besser die nächste Stufe von 40 Gbit/s möglich machen. Was bedeutet dies für die Komponenten? Zunächst einmal wird kein Weg am geschirmten Kabel vorbeigehen, die Standards der Kategorie 7 sind nur für paarweise geschirmte Kabel spezifiziert. Das ist für Verkabelungen gerade im deutschen Raum kein so großes Problem, da dies bisher ohnehin für die meisten Installationen ein De-Facto-Standard war bzw. ist. Aus dem großen Portfolio der geschirmten Kabel (Achtung: Kategorie 6 bzw. Kategorie 6A sind auch als ungeschirmte Variante verfügbar) gibt es die Wahlmöglichkeit zwischen

- Kategorie 6 (spezifiziert bis 250 MHz),
- Kategorie 6A (spezifiziert bis 500 MHz),
- Kategorie 7 (spezifiziert bis 600 MHz),
- Kategorie 7A (spezifiziert bis 1000 MHz).

Es ist allgemein bekannt, dass die höchste Bandbreite in der Regel auch die höchste Datenrate zulässt. Bei gleichen Preisen bezogen auf die Kabellänge bietet es sich deshalb an, den hochwertigsten Typ, also den Typ Kategorie 7A zu bevorzugen, sofern dieser keine weiteren bedeutenden Nachteile hätte. Der einzige nennenswerte Nachteil dieses Typs im Vergleich zu den „niederwertigen“ Typen besteht im ca. 2 mm größeren Außendurchmesser, dies verschlechtert theoretisch die Verlegeeigenschaften und führt zu größeren Kabelführungssystemen. Beides könnte im Prinzip die Kosten erhöhen, die Erfahrung von vielen Ausschreibungen zeigt aber, dass die Anbieter in den seltensten Fällen einen Mehrpreis für die Verlegung von höherwertigen Kabeln beanspruchen. Auch Kabelführungssysteme werden in der Regel bei Kategorie 7(A)- oder Kategorie 6(A)-Medien nicht unterschiedlich geplant. Damit gibt es keinen prägnanten Nachteil bei der Installation von höchstwertigen Kabeln im Rechenzentrum, gegebenenfalls bringt eine Ausschreibung mit alternativen Positionen für das einzelne Projekt Gewissheit bezüglich des Preisunterschiedes.

Die „Steckerfrage“ dagegen ist schwieriger zu lösen. Für den Fall, dass man sich konsequent für eine Verkabelung der Klasse F oder Klasse FA entscheidet, bleibt lediglich die Wahl zwischen dem TeraTM-Steckgesicht und dem GG45-Steckgesicht. Der Vorteil der GG45-Buchse besteht in der Kompatibilität zu vorhandenen RJ45-Anschlussschnüren, bis zum ersten Einsatz des Links für Klasse F(A) können alle bisherigen Schnüre weiterverwendet werden. Doch vergleichende Ausschreibungen, bei denen eine Kategorie 6A-Technik und eine GG45-basierende Technik gegenübergestellt wurden, zeigten, dass der Einsatz des GG45 zu einem ca. 3-fach höheren Preis der gesamten Anschlusstechnik führt (wohlgemerkt: Faktor 3 bei Material und Montage!) und dies damit das „Aus“ für viele Auftraggeber mit sich brachte. Der Mehrpreis des Tera-Systems ist nicht so hoch, dafür zwingt dieses System zum sofortigen Einsatz von Adapterschnüren (Tera auf RJ45), auch diese Einschränkung wird von Vielen nur ungern akzeptiert. Einen Ausweg aus diesem Dilemma bieten „modulare“ Lösungen, die einen einfachen Austausch der Buchse erlauben, dazu zwei Beispiele:

- Die Firma Tyco bietet seit vielen Jahren mit dem bewährten ACO-System eine modulare Technik an, die es ohne Spezialwerkzeug erlaubt, an das vorhandene Kabel eine (fast) beliebige Buchse anzuschließen, selbst Doppelbuchsen können zwecks CableSharing angeschlossen werden. Dazu werden einfach nur die im Anschlussblock eingesteckten Module ausgetauscht. Nach Aussage von Tyco ist dieses System Kategorie 7A-tauglich (angeboten werden GG45 und Tera). Leider benötigt das System im Rangierfeld viel Platz, so dass die Packungsdichte bei weitem nicht so hoch ist wie bei herkömmlichen Keystone-Lösungen (Keystone-Lösung: Das TP-Kabel wird mit einer einzelgeschirmten Buchse abgeschlossen).
- Die Firma LEONI Kerpen bietet mit dem Vario-Keystone eine ebenfalls modulare Lösung an. Das Kabel wird mit einem „neutralen“ Modul abgeschlossen, in welches dann wahlweise ein RJ45-Adapter (in unterschiedlichen Qualitäten) oder eine Tera-Buchse eingesteckt werden kann. Hier ist die Packungsdichte wesentlich besser als beim ACO-System. (siehe Abbildung 8)

Beide Systeme erlauben eine nachträgliche Änderung der Anschlusstechnik, ohne dass ein speziell ausgebildeter Monteur Montagearbeiten am Kabelende vornehmen muss. Doch es bleibt weiterhin die Frage offen, ob es überhaupt ein Verkabelungssystem der Kategorie 7A sein muss oder ob nicht ein kostengünstigeres System der Kategorie 6A ausreicht, welches immerhin auch für 10 Gbit/s nutzbar ist. Bedingt durch die kostengünstigere Anschlusstechnik stellt diese niederwertigere Variante eine sinnvolle Variante dar. Die Entscheidung hängt unter anderem davon ab, wie statisch die Verkabelung im Rechenzentrum ist. Ist zu erwarten, dass sich die Position der Serverracks oder gar der Bereichsverteiler sehr häufig ändert, so wird man ohnehin davon ausgehen, dass die Twisted-Pair-Verkabelung ebenso häufig erneuert werden muss. Ein Zurückziehen von vorhandenen Installationskabeln mit anschließender Neuverlegung derselben ist mit Standardinstallationskabel nicht zu empfehlen, dazu sind diese zu steif. Da

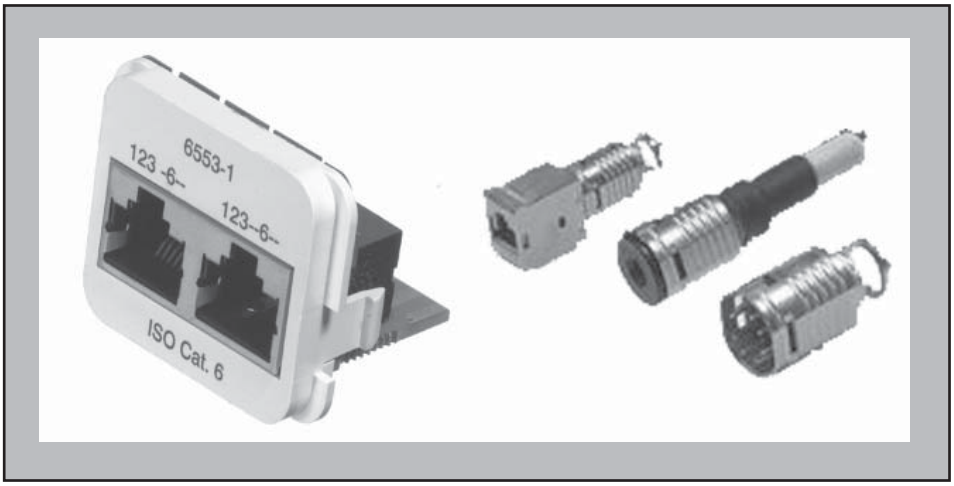


Abbildung 8: ACO-System Tyco Electronics und Variokeystone-System

somit nur eine Neuverkabelung möglich ist, besteht keine Notwendigkeit nach einem Verkabelungssystem, welches 10 bis 15 Jahre halten muss und damit eventuell eine Datenrate von 40 Gbit/s oder mehr bereitstellen muss. Man wird also in Abhängigkeit der aktuell benötigten Datenrate das Verkabelungssystem auswählen. Darin unterscheidet sich dieser Planungsansatz im Vergleich zur Tertiärverkabelung eines Gebäudes, diese Verkabelung ist statisch und wird unabhängig von der aktuell benötigten Datenrate geplant und realisiert. Plant man dagegen die Einrichtung eines Rechenzentrums, bei dem sich die Position der Datenanschlüsse mittel- und langfristig nicht ändert, wird sich der Einsatz einer Kategorie 7A-Verkabelung (inklusive Kategorie 7A-Anschlusstechnik) eher lohnen.

Vorteile von Plug-and-Play-Lösungen

Erwartet man ein dynamisch sich änderndes Rechenzentrum, gibt es weitere Herstellerkonzepte, die entscheidende Vorteile bringen können. Diese Konzepte vermeiden die Notwendigkeit einer Installationsausführung durch Fachfirmen. Alle bisher beschriebenen Installationen (LWL und Kupfer) setzen voraus, dass ein Installationskabel verlegt und dieses an beiden Enden mit Steckern konfektioniert wird. Die Konfektionierung erfordert ein sehr hohes Maß an handwerklichem Know-How und ist in der Regel Fachfirmen vorbehalten. Schnelle und spontane Änderungen der Positionen von Anschlüssen im Rechenzentrum sind nur bedingt möglich und entsprechend teuer. Die meisten Hersteller von Verkabelungssystemen bieten als Alternative Systeme an, die aus folgenden Einzelkomponenten bestehen:

- Mehrfachkabel bestehend aus mehreren Twisted-Pair-Kabeln oder mehrfaserigen Kabeln, beide Enden abgeschlossen mit normalen Steckern oder auch einem einzigen herstellerspezifischem Spezialstecker. Der Hersteller liefert ein Messprotokoll für alle Verbindungen mit.

- Modulare „Anschlussblöcken“, die im Schrank mit Hilfe von 19“-Technik oder auch in speziellen Doppelbodensystemen befestigt werden können. Eingangsseitig können auf diesen Block die Mehrfachkabel über den Spezialstecker angeschlossen werden und ausgangsseitig stehen dann ganz normale RJ45-Buchsen oder auch LWL-Kupplungen zur Verfügung.

Die daraus entstehenden Vorteile sind:

- Die Kabel können durch eigenes Betriebspersonal selbst verlegt werden und auch der Anschluss an die Anschlussblöcke kann ohne großartige Fachkenntnisse selbst durchgeführt werden (einfaches Aufstecken).

- Im Falle von Änderungen der Positionen der Anschlüsse lassen sich die Änderungen der Verkabelung selbst durchführen, spezielle Installationsunternehmen sind nicht notwendig.

Dagegen gibt es neben der Herstellerabhängigkeit allerdings einen Nachteil der gerade in Zusammenhang mit der oben geführten Diskussion zu berücksichtigen ist: Bei Kupfer sind derzeit keine oder nur sehr wenige Systeme mit Kategorie 7(A)-Qualität auf dem Markt verfügbar. Damit verliert diese Lösung an Attraktivität für eine kupferbasierende Rechenzentrumsverkabelung, die mehr als 10 Gbit/s sicherstellen soll. (siehe Abbildung 9)

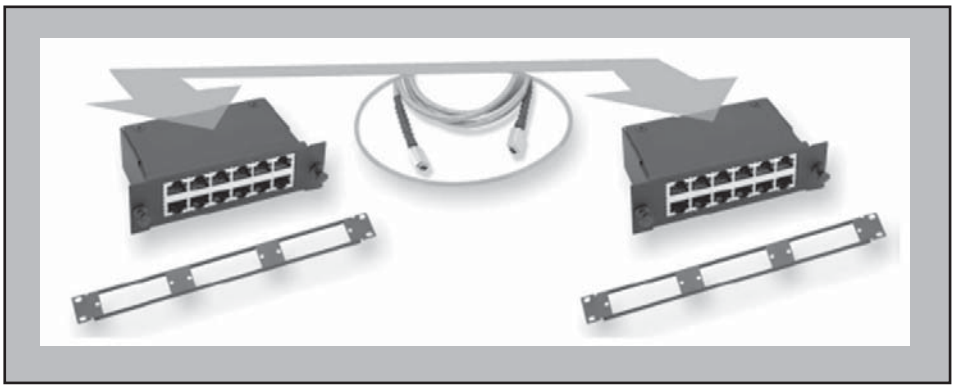


Abbildung 9: Beispiel MRJ21 von Tyco Electronics

Zusammenlegung von Rechenzentrum und Etagenverteiler

Bei der Neuplanung von Etagenverteilern im Rahmen eines Verkabelungs-Redesigns wird sehr gerne ein neuer Etagenverteiler in das Rechenzentrum oder den Serverraum platziert. Dies bietet den Vorteil der Nutzung einer in der Regel vorhandenen guten Infrastruktur mit Doppelboden, Kühlung, USV-Versorgung etc. Moderne EMV-gerechte Konzepte raten jedoch davon ab, wenn Kupfer als Tertiärmedium genutzt wird. Der Grund liegt darin, dass diese modernen EMV-Konzepte von der Einteilung eines Gebäudes in unterschiedliche Blitzschutzzonen ausgehen. Im äußeren Bereich des Gebäudes (Blitzschutzzone 0) wird die durch indirekten Blitzeinschlag entstehende Überspannung am größten sein und zu einem sehr hohen Induktionsstrom führen. Metallene Leitungen, die von außen in ein Gebäude eingeführt werden, führen vereinfacht gesagt diesen hohen Strom ins Gebäude (Blitzschutzzone 1). Deshalb sieht man z.B. in der klassischen Telefonverkabelung am Gebäudeeintritt einen so genannten Überspannungsschutz vor. Im Gebäude selber gibt es aber ebenfalls weitere Zonen, die mit diesem hinter dem Überspannungsschutzelement noch verbleibenden Reststrom ein Problem hätten, elektronische Komponenten könnten durch diesen Strom zerstört werden. Das hat zur Folge, dass weitere Blitzschutzzonen definiert werden und der ausgangsseitig am Überspannungsschutzelement in die nächste Zone übrige bleibende Strom immer kleiner wird. Server-Einheiten eines Rechenzentrums haben einen sehr hohen Schutzbedarf haben, man „packt“ sie in die Blitzschutzzone 2 und muss deshalb dafür Sorge tragen, den Reststrom des Blitzes in das Rechenzentrum hinein zu minimieren. Normgerechte Konzepte sehen deshalb vor, jeden metallischen Leiter, der in oder aus dem Rechenzentrum geführt wird, mit einem Überspannungsschutzelement zu sichern. Würde das Rechenzentrum einen Etagenverteiler mit TP aufnehmen, so müssten demzufolge alle TP-Leitungen jeweils mit einem Überspannungsschutzelement in der passenden nachrichtentechnischen Qualität abgesichert werden (Anbieter z.B. die Firma Phoenix). Das wird zwar bei der Datenverkabelung sehr selten praktiziert (bei der Stromverkabelung dagegen schon!), was aber nicht heißt, dass dieses Risiko deshalb nicht existiert. Bei Aufbau eines hochverfügbaren Rechenzentrums wäre eine Missachtung dieses als allgemein etablierten Blitzschutzzonenkonzeptes (DIN EN 62305 (VDE 0185-305) fahrlässig und die Platzierung eines Etagenverteilers sollte deshalb nach Möglichkeit nicht im Rechenzentrum vorgesehen werden.

IT-Verkabelung im Rechenzentrum: Beginn einer neuen Epoche?

Kabelführungssysteme und Dokumentation

Die Kabelführung in vielen „historisch gewachsenen“ Rechenzentren und Serverräumen darf als katastrophal bezeichnet werden. Dies ist bedingt durch zwei Versäumnisse:

- Die Installation einer „strukturierten Verkabelung“ im Rechenzentrum ist im Prinzip erst eine „neuzeitliche“ Idee. Lange Zeit wurden die Anschlüsse der Server mit Hilfe von spontan im Doppelboden eingezogenen Anschlussschnüren zwischen den Servern und den Switches hergestellt. Eine Infrastruktur an Kabelführungssystemen im Doppelboden war bzw. ist nicht vorhanden und eine „Kreuz-und-Querverkabelung“ ist die Konsequenz.

- Die verlegten Anschlussschnüre wurden in vielen Fällen nicht oder nur mangelhaft dokumentiert, so dass ein Entfernen von nicht mehr benötigten oder defekten Anschlussschnüren unmöglich war.

Das Ergebnis besteht sehr häufig in einem völlig überfüllten Doppelboden. Dabei ist die Kabelführung im Prinzip nur eine zusätzliche Funktion des Doppelbodens im Rechenzentrum, in den meisten Rechenzentren wird dieser Doppelboden ebenfalls für die Belüftung der Serverschränke benötigt. Gerade in Anbetracht der immer größeren Kühlleistungen für die Systeme steigt die Bedeutung eines möglichst ungehinderten Luftstromes im Doppelboden und jede Art von Chaos-Verkabelung beeinträchtigt dies. Eine Dimensionierung des Luftstromes durch Klimatechniker wird bei sich ständig verändernder Verkabelung nur schwer möglich sein. Diese Vermeidung spricht für volumensparende Verkabelungstechniken wie Glasfaser oder „Vielfachkabel“, sie zwingt aber auch zur Benutzung von Kabelführungssystemen. Dabei müssen diese in erster Linie zur Verlegung der festinstallierten Kabel verwendet werden, und nach Möglichkeit sind alle Rangier- und Anschlussschnüre aus dem Doppelboden herauszuhalten. In kleineren Rechenzentren oder gar Serverräumen mag die direkte Verlegung der Kabel auf den festen Boden akzeptabel sein, aber auch hier wird empfohlen Kabelführungssysteme wie Trasse oder Gitter vorzusehen. Diese sichern zum einen eine geordnete Kabelführung, verhindern einen Wildwuchs und zum anderen schützen sie auch die verlegten Kabel. Welches System bietet hier wo Vorteile?

Einsatz einer Trasse: Eine Trasse hat den Vorteil, dass der mechanische Schutz der Kabel besser ist. Nach den Ergebnissen einer Untersuchung der Labore Labors, AEMC Mesures und CETIM bietet eine Trasse nicht grundsätzlich einen besseren elektromagnetischen Schutz als eine Gitterrinne, in Abhängigkeit des gewählten Produktes für die Gitterrinne bewirken beide den gleichen „Faradayschen Käfig“-Effekt (Quelle: www.cablofil.at). Als wichtiger Nachteil ist zu nennen, dass nur dann eine Trasse zu empfehlen ist, wenn die Ein- und Ausfädelungspunkte durch Ausschnitte an der Trasse mit entsprechendem Kantenschutz eine Beschädigung der Kabel verhindert. Bei nachträglich neu vorzusehenden Ausfädelungspunkten wird dieser dann neu zu machende Ausschnitt sehr schwierig und eine Beschädigung der Kabel droht. Für den Fall eines zusätzlichen Deckels wird die Gefahr verringert, dass „Fremdkabel“ wie z.B. Starkstromleitungen im Rahmen von Nachverkabelung auf die Datenkabel verlegt werden können und diese beeinträchtigen.

Einsatz einer Gitterrinne: Eine Gitterrinne bietet nicht den gleichen mechanischen Schutz, die Auflagepunkte der Kabel auf die Gitterstäbe können bei hoher Kabeldichte die unteren Kabel mechanisch beeinträchtigen. Dieses Risiko kann deutlich vermindert werden, wenn auf den Boden der Rinne eine Blechplatte gelegt wird, die den Punktdruck der Kabel vermeidet. Der Vorteil der „offenen“ Gitterrinne besteht in der besseren Möglichkeit zur Ausfädelung der Kabel. Die Möglichkeit zur Verwendung eines zusätzlichen Deckels stellt bei Gitterrinnen eine Ausnahme dar, ist aber bei einzelnen Herstellern ebenfalls möglich. (siehe Abbildung 10)

Gibt es also passende Lösungen für die Verlegung von Installationskabel, so bleibt die Frage: Wohin mit den Anschlussschnüren, wenn nicht in den Doppelboden? Ein Vergleich der Verteilerelemente aus der EN 50173-1 und EN 50173-3 macht die Idee und damit die Lösung des Problems noch mal deutlich: Der Bereichsverteiler übernimmt im Prinzip die Funktion des Etagenverteilers und das Element GA (im Verteilerschrank) übernimmt die Funktion der „Anschlussdose“ (entsprechend in einem Raum). Diese „Anschlussdose“ befindet sich in einem Schrank, der im Prinzip vergleichbar ist zu einem Büroraum. Niemand käme auf die Idee, in einem Büro grundsätzlich von einer Dose aus mit einer langen Anschlussschnur einen anderen Raum zu versorgen. Genauso sollte im Rechenzentrum von einem GA aus nur ein Element im gleichen Schrank versorgt werden. Befolgt man diesen Grundsatz, so wird es keine oder zumindest eine deutlich geringere schrankübergreifende Verkabelung mit Anschlussschnüren geben und der Doppelboden bleibt von diesen verschont. Natürlich können schrankübergreifende Anschlussschnüre nicht vollkommen ausgeschlossen werden, dies sollte aber dennoch außerhalb des Doppelbodens erfolgen. Dazu stehen 3 nennenswerte technische Varianten zur Verfügung:

- Realisierung von Trassen bzw. Gitterrinnen oberhalb der Schränke. Die Vor- und Nachteile der beiden Systeme wurden bereits oben für die Montage im Doppelboden beschrieben.

- Die deutlich elegantere - aber auch kostenaufwendigere - Alternative zu Trassen bzw. Rinnen sind spezielle Wannensysteme zur Kabelführung, wie z.B. das durch seine knallgelbe Farbe auffallende System FiberRunner von Panduit, welches ebenfalls oberhalb der Schränke montiert wird. Dieses System bietet eine Vielzahl von Formstücken (z.B. T-Stücke, Ausfädelungsstücke etc.), die zusammengesteckt werden und insbesondere für eine Einhaltung der Biegeradien an den Kabeln sorgen.

- Fehlt die Möglichkeit zur Montage von zusätzlichen Kabelführungssystemen

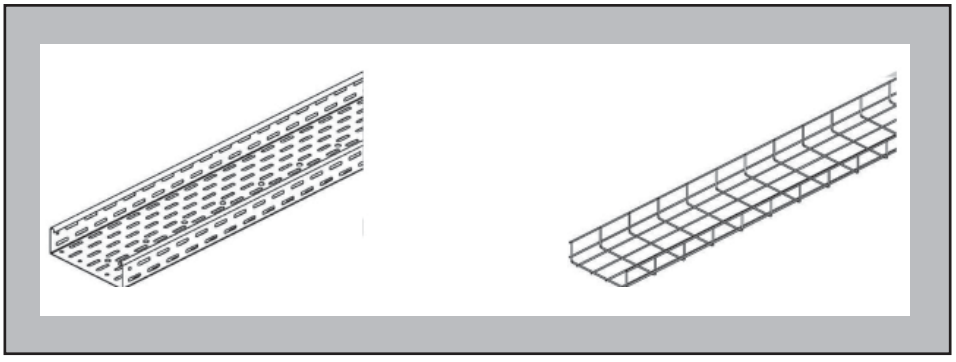


Abbildung 10: Kabeltrasse und Gitterrinne

oberhalb der Schrankreihe, so bietet teilweise die nachfolgend beschriebene einfache Maßnahme innerhalb der Schrankreihe enorme Vorteile. Zieht man in jedem Schrank der Reihe an der gleichen Höheneinheitenposition eine Kabelführung mit Hilfe von Kabelführungswannen – keine Kabelführungsplatten mit Ösen - vor (Höhe der Wanne am besten 2 HE), so entsteht dadurch eine durch die Schrankreihe laufende Kabelführungswanne, die sehr gut zur schrankübergreifenden Verlegung von Anschlussschnüren genutzt werden kann. Sehr häufig wird diese „Kabelführungsreihe“ im unteren, mittleren und oberen Bereich montiert, so dass hier eine saubere und nicht überfüllte Kabelführung möglich wird.

Die beschriebenen technischen Maßnahmen zur Errichtung von Kabelführungssystemen sind mit Sicherheit nicht unbedingt neu, deren Einsatz im Rechenzentrum dagegen wirkt vielfach jedoch noch befremdlich. Auch dies ist im Zusammenhang mit einer strukturierten Rechenzentrumsverkabelung noch zu lernen.

In Zusammenhang mit der neuen Art der Rechenzentrumsverkabelung kommt ein neuer Aspekt bezüglich der Dokumentation der Verkabelung eines Rechenzentrums hinzu. Gibt es reichliche Richtlinien zur Dokumentation von Verkabelungselementen im Standardgebäude, so greifen diese Regeln im Rechenzentrum häufig nicht mehr. Bereits die Tatsache, dass ein Rechenzentrum ein einziger großer Raum ist und damit eine raumbezogene Dokumentation bzw. Nummerierung der Komponenten nicht mehr sinnvoll ist, zeigt, dass hier ein neuer Lösungsansatz notwendig ist. Eine interessante Strategie sieht vor, das Raster des Doppelbodens für die Zuordnung von Elementen zu nutzen. Man überzieht den Raum mit einem XY-Raster passend zu den Doppelbodenplatten. Jeder Schrank lässt sich somit einer XY-Koordinate zuordnen und die im Schrank enthaltenen Elemente können dann über diese Koordinate leicht lokalisiert und dem Beschriftungsschema zugeordnet werden.

Fazit

Trotz der Gültigkeit der EN 50173-3 für die Rechenzentrumsverkabelung ist davon auszugehen, dass eine Verkabelung nach oder in Anlehnung an diese Norm nicht den gleichen Nutzbarkeitszeitraum sicherstellen muss und wird, wie dies im Gebäudebereich über die EN 50173-1 gefordert wird. Konzepte mit bedarfsorientierter Verkabelung und daraus sich ableitendem verändertem Design und Materialauswahl dürfen nicht als falsch dargestellt werden, sie stellen eine Alternative dar und werden gerade bei kleineren Rechenzentren oder Serverräume eine vernünftige Option sein. In diesem Falle gibt es keine Notwendigkeit zum Einsatz von Lösungen mit extrem hochwertigen Steckersystemen, die nur von wenigen Herstellern angeboten werden und eine Abhängigkeit von diesen bedingt (Beispiel GG45). Hier können weiter verbreitete und kostengünstigere Systeme wie Standard-RJ45 in Kategorie 6A-Qualität oder auch „nur“ Kategorie 5-Qualität sinnvoller sein. Mit zunehmender Größe eines Rechenzentrums müssen diese geplant werden wie eigene Gebäude in einem Gebäude und eine strukturierte, statische Verkabelung wird - zumindest zwischen den Verteilern - wahrscheinlicher. Dies spricht für Langzeitlösungen und damit auch für höhere Qualitäten, wie sie z.B. durch Kategorie 7A oder auch durch Glasfaser eher sichergestellt werden können. In allen Fällen ist dafür zu sorgen, dass Kapazität (im Sinne von Übertragungsrate) nicht zwangsläufig höher bewertet wird als Flexibilität. Gerade eine gute Anschlusstechnik muss sicherstellen, dass schnelle Änderungen oder auch schnelle Reparaturen mit Standardmaterialien möglich sind, nur so können die verlangten hohen Verfügbarkeiten sichergestellt werden.

Für den Vergleich Kupfer versus Glasfaser gibt es im Rechenzentrum technische Vorteile der Glasfasertechnik, doch in der Vergangenheit hat sich immer wieder gezeigt, dass die Schnittstelle an den Endgeräten die Technik bei der Verkabelung vorgibt. Eine gut gemeinte „erzwungene“ Glasfaserverkabelung wird bei fehlenden Schnittstellen an den Servern auf wenig Akzeptanz stoßen und ist deshalb meistens nicht haltbar. Damit liegen (leider) die Vorteile auf Seiten der Kupferlösungen. Doch dies bedeutet nicht den völligen Verzicht auf Glasfaser, wie gezeigt wird es auch in größeren Rechenzentren mehrere Verkabelungshierarchien geben und für die Hierarchieebene Hauptverteilungsverkabelung ist die Glasfaser prädestiniert. Im Falle einer von einem Punkt ausgehenden zentralen Verkabelung ist ab einer bestimmten Größe des Raumes die Glasfaser nicht vermeidbar.

Neues Seminar

Unified Communications mit Siemens - HiPath 8000 & OpenScape im Überblick

Die ComConsult Akademie veranstaltet vom 25. - 26.05.09 erstmalig ihr neues Seminar „Unified Communications mit Siemens - HiPath 8000 & OpenScape im Überblick“ in Hamburg.

Mit der Zusammenführung der rein SIP-basierten TK-Lösung HiPath 8000 und der Applikation-Suite OpenScape präsentiert Siemens ein umfangreiches Kommunikationsprodukt, das verspricht, im Sinne von Unified Communications alle modernen Kommunikationstechnologien unter einer gemeinsamen Struktur für den Endanwender steuerbar und nutzbar zu machen. So wurden neben der in der Tradition der bekannten HiPath-Telefonanlagen stehenden Sprachlösung weitere Dienste und Leistungsmerkmale wie Präsenzanzeige, Erreichbarkeitsanzeige, regelbasierte automatische Steuerung der Erreichbarkeit, Instant Messaging, Fax und E-Mail sowie Webkollaboration und Videokonferenzsysteme integriert.

Gelingt mit OpenScape der Einstieg in eine Welt, in der alle verfügbaren Kommunikationstechniken einfach, schnell und situationsgerecht eingesetzt werden können?

Schon allein aufgrund des signifikanten Marktanteils von Siemens Enterprise TK-Lösungen im europäischen Markt kommen

Projektentscheider, TK- und IT-Verantwortliche kaum um eine nähere Betrachtung dieses Produktes herum.

Das Seminar behandelt daher die folgenden Punkte:

- Was versteht man bei SEN unter präsenzbasierender Kommunikation?
- Aus welchen Modulen besteht die OpenScape Suite?
- Wie passt sich die Lösung den heutigen Architekturanforderungen an?

Weitere Schwerpunkte sind zudem:

- Welche SIP Standards und Leistungsmerkmale werden unterstützt?
- Wie verhält sich die Lösung bei der Benutzerverwaltung und dem Aufbau von Wählplänen?
- Welche zusätzlichen Dienste wie z.B. ACD oder Voicemail werden vom Basismodul unterstützt?
- Wie ergänzen zusätzliche Produkte wie Xpressions (Voicemail) und Enterprise Mobility die Siemens Lösung?
- Welche Funktionen werden von den Soft- & Webclients, sowie den SIP Desktopendgeräte abgedeckt?
- Wie unterstützt die UC-Lösung die Integration von 3rd Party Endgeräten?

Dieses Seminar soll einen gezielten Überblick über die Leistungsfähigkeit der Siemens Enterprise Communications Lösung vermitteln. Es richtet sich daher an Entscheider und Architekten, die eine Bewertungs- und Entscheidungshilfe zur Realisierung von TK-Projekten wünschen.

Unsere herstellerunabhängigen und neutralen Experten haben sich sehr ausführlich mit den technischen Details befasst und verfügen über langjährige Erfahrung bei der Implementierung und der Konzeption von TK-Lösungen sowie bei der Bewertung von Kommunikationstechnologien.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Unified Communications mit Siemens - HiPath 8000 & OpenScape im Überblick

Ich buche das Seminar
Unified Communications mit Siemens - HiPath 8000 & OpenScape im Überblick
☐ 25.05. - 26.05.09 in Hamburg

☐ Bitte reservieren Sie für mich ein Hotelzimmer

vom_____ bis_____09

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

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

Schwerpunktthema

Dipl.-Inform. Oliver Flüs verfügt über langjährige Kenntnisse im Betrieb von IT-Infrastrukturen. Als Leiter des Competence Center IT-Service der ComConsult Beratung und Planung GmbH bearbeitet er seit Jahren Projekte in den Bereichen Services im IT-Bereich. Zu diesen Themengebieten ist er regelmäßig als Referent bei der ComConsult Akademie tätig, unter anderem als Schwerpunktreferent zu TCP/IP-Aspekten, in der Trouble Shooter-Seminarreihe sowie im Rahmen der Sicherheitsseminare.

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

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: Sicherheit in virtuellen Server-Umgebungen

Fortsetzung von Seite 1

1. Auswirkungen auf die IT-Landschaft

Die Auswirkungen der Server-Virtualisierung auf die administrativen und betrieblichen Prozesse können erheblich sein. So werden womöglich durch die Server-Virtualisierung Ressourcen zusammengeführt, die im Unternehmen oder der Behörde bisher zum Teil durch verschiedene Verantwortungsbereiche abgedeckt werden, z.B. Server- und Netzbetrieb. Server- und auch Netzkomponenten sind virtualisiert innerhalb von physischen Servern untergebracht. Hierbei gilt es vor allem die Frage der Zuständigkeiten zu klären. Bisher bewusst getrennte Rollen und Kontrollfunktionen fallen nun zusammen und betreffen den Netz- und Server-Betrieb genauso wie die IT-Sicherheit oder Revision. Hinzu kommt der Betrieb der Virtualisierungslösung selbst: Wird diese vom Server-Betrieb gepflegt oder durch einen anderen, ggf. eigenen Bereich? Aus einer Sicherheitsperspektive sind dabei unmittelbar die potentiellen Zugriffsmöglichkeiten der Virtualisierungsadministratoren zu berücksichtigen, die ohne differenzierte Berechtigungskonzepte eine umfassende Kontrolle über eine Vielzahl von Servern erhalten.

Wirtschaftliche Aspekte dominieren die Server-Virtualisierung

Die Server-Virtualisierung findet aufgrund der vordergründigen wirtschaftlichen Thematik „Einsparung von Hardware“ häufig schneller Einzug in das Rechenzentrum als es dem IT-Betrieb unter Umständen lieb ist. Die Verantwortlichen sind sich dabei oft nicht aller Konsequenzen bewusst. Mit Erfahrung beherrschte Szenarien auf Basis dedizierter physischer Server werden durch den neuen Ansatz der Virtualisierung zum Teil im Rekordtempo abgelöst. Die neu eingeführte Technik mit gleicher Qualität zu beherrschen wie die „althergebrachte“ ist zwar nicht unmöglich, erfordert aber Einarbeitungszeit und Tests, für welche die beobachteten typischen Einführungsphasen oft zu kurz sind. In dieser Zeit kann man bestenfalls an der Oberfläche des nötigen Wissens gekratzt haben, bis die virtualisierte Lösung in den produktiven Betrieb geht.

Dabei birgt eine derart weitgehende Umstellung im technischen Bereich auf Grund der in heutigen IT-Umgebungen zwangsläufigen Vielzahl von Abhängigkeiten etliche Risiken – nicht zuletzt auch aus sicherheitstechnischer Sicht. Von der Virtualisierung sind neben den technischen Aspekten sowohl IT-Betriebsprozesse als auch Geschäftsprozesse betroffen. Für alle diese Bereiche stellen sich bekannte Fragen im Sinne des Risiko- und insbesondere Sicherheitsmanagements neu. Beispielsweise sind veränderte Deployment-Prozesse ebenso zu berücksichtigen wie geeignete Maßnahmen zur Absicherung einer SAN-Umgebung. Diese Punkte müssen in bestehende Sicherheitskonzepte eingearbeitet oder in Form eines Sicherheitskonzepts für die Virtualisierung berücksichtigt werden, denn trotz

gewisser Analogien können die bisherigen Konzepte nicht unverändert übernommen werden. Anschließend müssen die Konzepte in geeignet modifizierten betrieblichen Abläufen im IT-Service umgesetzt werden. Nur bei Berücksichtigung dieser Aspekte können die Vorteile der Virtualisierung sinnvoll in die Umgebung integriert werden. Bei Nichtbeachtung bzw. diesbezüglich unzureichender Vorbereitung droht hingegen ein deutlicher Abfall des verantwortlich garantierbaren Sicherheitsniveaus.

Virtualisierung: Gemeinsame Nutzung von Ressourcen

Das Sicherheitsniveau ist in virtualisierten Umgebungen zunächst durch die Schwächung eines der Grundpfeiler der IT-Sicherheit betroffen, nämlich der konsequenten Trennung von Ressourcen bei hohen oder unterschiedlichen Anforderungen an Verfügbarkeit, Integrität und Vertraulichkeit von gespeicherten oder im Rahmen von Kommunikationsflüssen transportierten Daten. Über Jahre hat es sich die IT-Sicherheit zur Aufgabe gemacht, über differenzierte Verfügbarkeitsbetrachtungen und nötigenfalls Unterscheidung verschiedener Sicherheitszonen Ressourcen zu isolieren und abzusichern, um die IT-Nutzer und ihre Daten auf diese Weise vor Angriffen zu schützen. Je höher die Ansprüche an Sicherheit im engeren Sinne oder Verfügbarkeit, umso wahrscheinlicher war der Einsatz dedizierter Hardware und separierter Kommunikationswege. Um das Risiko „Mensch“ zu minimieren, ging dies oft mit einer Verteilung der Administrationsrechte für unterschiedliche Systeme auf unterschiedliche Verantwortliche einher.

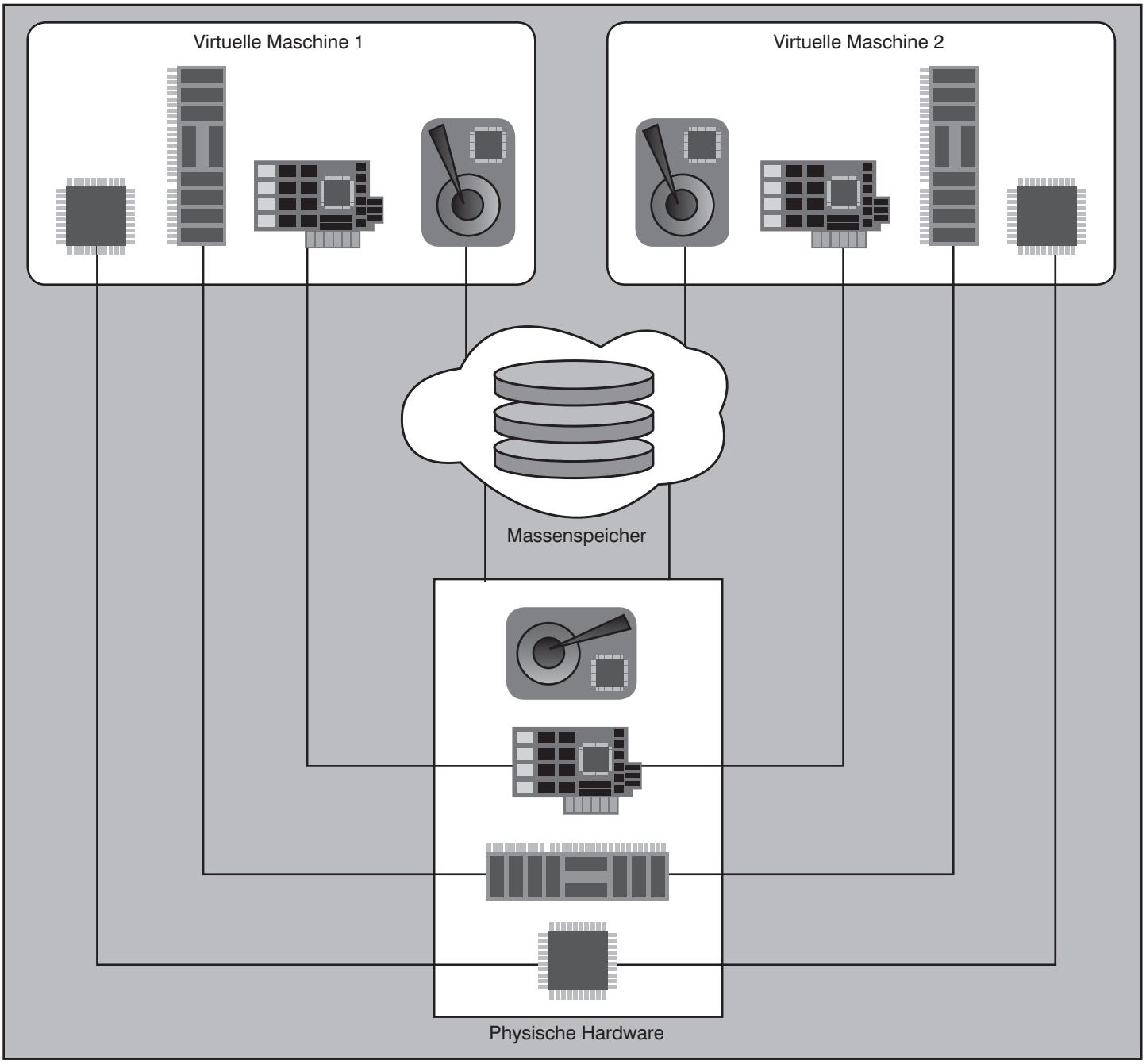


Abbildung 1: Ressourcenteilung zwischen physischen und virtuellen Systemen

Virtualisierung: Sicherheit in virtuellen Server-Umgebungen

Zusammen mit der Einführung einer Server-Virtualisierung werden Hardware-Ressourcen jedoch wieder zusammengeführt. Damit wird die vorhandene physische Hardware nicht länger einem System dediziert zur Verfügung gestellt, sondern wird potentiell von mehreren Systemen (Abbildung 1) genutzt. Die Verwaltung obliegt einer Software, die zur Virtualisierungsbasis gehört. Wenn die bisherigen Separierungsstrategien nicht völlig widersinnig waren, ergeben sich bei diesem rückwärtigen Schritt zur gemeinsam genutzten Basisplattform sofort gezielte Fragen. Hinzu kommt die ständig zunehmende Komplexität der IT-Systeme, deren Beherrschung durch den Übergang von physischen zu virtuellen Systemen nicht erleichtert wird, denn Virtualisierung bringt einen erhöhten Abstraktionsgrad in IT-Planung und Betriebsalltag. Endet dies in einem Verlust von Transparenz und Überblick, ist ein gezielter Umgang mit Sicherheitsrisiken fraglich - hier muss man sich vorsehen!

2. Grundlage Risikoanalyse

Das nicht selten vorzufindende Argument, dass eine Virtualisierung zu mehr Sicherheit führe, gilt per se nicht. In diesem Zusammenhang wird oft das Beispiel angeführt, dass es sicherer sei, einen physischen Server mit drei virtuellen Servern und je einem Dienst zu betreiben als einen physischen Server mit drei Diensten. Das für die Betrachtung korrekte physische Pendant zum genannten virtuellen Szenario besteht jedoch aus drei physischen Servern mit je einem Dienst, sollen nicht die berühmten Äpfel und Birnen verglichen werden. Mindestens aus Sicht der Streuung des Ausfallrisikos sind drei dedizierte physische Server die sicherste Lösung. Die maximale Separierung in unterschiedliche Sicherheitszonen setzt ebenfalls eine solche Konstellation voraus. Doch damit soll diese Art der Diskussion auch ein Ende haben: Pauschalitäten dieser Art führen in der IT-Praxis zu nichts.

Der Sicherheitsanspruch und der Einsatz von Mitteln müssen stets in ein zum konkreten Bedarf passendes gesundes Verhältnis gesetzt werden. Damit ist keine Lösung in jedem Fall sofort „die bessere“. Begrenzte Ressourcen bei Geld und Personal sind abzuwägen, und die Bewertung des erreichten oder erreichbaren Sicherheitsniveaus hängt auch in virtuellen Umgebungen von diversen Faktoren ab (siehe auch BSI IT-Grundschutz-Kataloge Maßnahme M 2.392 „Sicherer Einsatz virtueller IT-Systeme“). Die Wahl der Technik ist dabei nur eine zu berücksichtigende Größe.

Grundsätzlich führt die Verkettung aus physischem und virtuellem System im ersten Schritt sowohl aufgrund der Architektur als auch der zusätzlichen Komplexität zu einem geringeren Sicherheitsniveau, da ein Mehr an Software-Komponenten auch ein Mehr an denkbaren Schwachstellen bedeutet. Inwiefern eine Lösung den Anforderungen genügt, muss bei jeder Technik über eine gezielte Risikoanalyse und hieraus hervorgehender Maßnahmenwahl sicher gestellt werden. Als Basis dienen hierzu eine umgebungsspezifische Festlegung konkreten Sicherheitsbedarfs sowie ein solides Wissen um die Prüfpunkte und Möglichkeiten der jeweiligen technischen Basis.

3. Gefährdungen und Maßnahmen

Insgesamt ist die logische Konsequenz des Wegfalls bzw. Ersatzes von Hardware eine deutliche Verschiebung der Risiken in Richtung Software. Teilweise können bestehende Konzepte und Best Practices zur IT-Sicherheit für virtuelle Server-Umgebungen übernommen werden; andere Bereiche müssen hingegen (wie im Folgenden beschrieben) neu erarbeitet oder zumindest angepasst werden.

Für die Absicherung der Umgebung, physisch wie virtuell, gelten im Allgemeinen die bisherigen Grundsätze, wobei zusätzliche Gefährdungen und entsprechende Maßnahmenkataloge berücksichtigt werden müssen.

Zu den Angriffsvektoren bzw. Risiken im Zusammenhang mit dem Einsatz einer Server-Virtualisierung zählen insbesondere die nachfolgenden Punkte. Zu unterscheiden ist dabei nach von einem Fehler betroffener Ebene der Virtualisierungslösung (bestehend aus der Hardware der Virtualisierungsbasis und der Software-Ebene der Virtualisierungsbasis, d.h. Host-System bzw. Hypervisor) und den auf dieser Basis laufenden virtuellen Servern. Je nach Zusammenwirken von verschiedenen Teillösungen aus Sicht des Anwenders kann sich dabei die Auswirkung auf ein Gesamtsystem aus verschiedenen, auf unterschiedlicher Hardware realisierten Servern erstrecken:

- Hardware → Host-System/Hypervisor

  Ein Fehler in der Hardware der Virtualisierungsbasis kann direkte Auswirkungen auf die Verfügbarkeit des Host-Systems haben und sich damit potentiell auf eine Vielzahl virtueller Server auswirken.

- Host-System/Hypervisor → virtuelle(r) Server

  Ein Fehlerzustand der Software der Virtualisierungsbasis (bei fehlerfrei funktionierender Hardware) kann je nach Umfang der betroffenen virtuellen Servern ein Gesamtsystem als Ganzes unbrauchbar machen (Beispiel: VMware ESX Lizenzfehler im August 2008[1]).

[1] siehe http://kb2.vmware.com/kb/1006716.html

- Virtuelle Maschine → andere virtuelle Maschine(n)

  Eine Überbeanspruchung von Ressourcen (ob beabsichtigt oder nicht) kann sich auch auf andere virtuelle Maschinen negativ auswirken, soweit die Virtualisierungsbasis hier keine strikt getrennte Ressourcenzuordnung realisiert. Auch können Fehler in der Virtualisierungssoftware einen Einbruch von einer virtuellen Maschine aus in eine fremde virtuelle Maschine begünstigen. Dies kann je nach Art und Umfang einen erfolgreichen Angriff auf eine einzelne virtuelle Serverlösung darstellen oder ein Gesamtsystem betreffen dem der angegriffene Server aus Anwendersicht angehört.

- Virtuelle Maschine → Host-System/Hypervisor

  Angriffe können weiterhin aus der virtuellen Maschine direkt auf den Hypervisor zielen und damit womöglich in der Kompromittierung des Gesamtsystems enden.

- Virtuelle Maschine → Storage

  Sofern die virtuelle Maschine Zugriff auf von mehreren Servern genutzten Storage hat, z.B. mittels iSCSI oder virtualisierten Host-Bus-Adaptern (HBAs), müssen Vorkehrungen getroffen werden, dass kein Zugriff auf fremde Datenbestände möglich ist. Diese Notwendigkeit gilt auch in nicht virtuellen Umgebungen, jedoch ist gemeinsame Nutzung gleicher Storage-Hardware in virtuellen Umgebungen typischer, womit dieser Gesichtspunkt stärker zu bewerten ist.

- Extern → Host-System/Hypervisor

  Angriffe von außen, die sich direkt an das Host-System richten, können im schlimmsten Fall ebenfalls eine vollständige Kompromittierung des Host-Systems bedeuten.

Diese Liste illustriert (ohne Anspruch auf Vollständigkeit) die Komplexität der Gefährdungslage. Hinzu kommen je nach Umgebung weitere Systeme, zu denen Abhängigkeiten bestehen. Im Folgenden werden die Herausforderungen an die IT-Sicherheit für die verschiedenen Bereiche der Server-Virtualisierung genauer betrachtet.

3.1 Überwachung innerhalb der Virtualisierung

Die „Verdichtung" der Infrastruktur erfordert nicht zwingend neue Werkzeuge, jedoch müssen bisher genutzte Werkzeuge der neuen Situation angepasst werden, um die Kontrolle über die IT-Landschaft zu behalten. Die Server-Infrastruktur endet durch den Einsatz der Virtualisierung nicht länger am physischen Server, der entsprechend im Monitoring und der Dokumentation (z.B. physisches und logisches Design) abgebildet werden muss. Die Notwendigkeit einer geeigneten Überwachung und Dokumentation gilt umso mehr in virtuellen Umgebungen, da sich die Server-Anzahl mit der Server-Virtualisierung erfahrungsgemäß erhöht. Die Gründe für erhöhte Server-Anzahlen liegen sowohl im einfacheren Deployment neuer Server z.B. für Test- und Entwicklungssysteme als auch in der Isolation von Diensten, die bisher auf einem gemeinsam genutzten physischen Server liefen.

Die genannten Aspekte zeigen bereits, dass dem Management und der Überwachung der virtuellen Infrastruktur besondere Aufmerksamkeit gewidmet werden muss. Die Herausforderungen liegen dabei in der hohen Dynamik einer virtuellen Infrastruktur, die bisher überwiegend statisch in Form von fest zugeordneten Ressourcen vorlag. Mittels dynamischer Verteilung von virtuellen Servern ist dieses Gesetz aufgehoben.

Neben der Virtualisierungsinfrastruktur selbst, die überwacht werden muss, sind Werkzeuge erforderlich, die den Datenfluss innerhalb der virtuellen Umgebung überwachen. Dieser Verkehr ist für klassische Monitoring-Lösungen, welche Daten an physischen Infrastruktur-Elementen ermitteln, unsichtbar (beispielsweise die Auslastung einzelner virtueller Switch Ports). Aber auch die Überwachung einzelner Applikationen und deren Performance bzw. Antwortzeit ist zu berücksichtigen, da die virtuelle Maschine sich eine gemeinsame physische Hardware mit weiteren virtuellen Maschinen teilen muss, die ebenfalls Einfluss auf die Leistung haben können. An dieser Stelle sind neue Mechanismen zur Ressourcenplanung und Kontrolle notwendig.

Da die meisten Funktionen in Form von Software abgebildet sind, ist auch das Risiko der Fehlbedienung höher, da beispielsweise das Kappen einer Netzanbindung, das Ausschalten von Servern oder der Rollback eines Snapshots nur weniger Mausklicks bedarf. Diese Risiken können durch angepasste und eingeübte Prozesse vermindert werden. Die größte Herausforderung besteht somit im Betrieb der Lösung.

3.2 Sicherheit des Host-Systems

Das Fundament der Server-Virtualisierung sind die Host-Systeme, auf denen die virtuellen Maschinen betrieben werden. Der oft thematisierte GAU besteht in der vollständigen Kontrolle des Host-Systems durch einen Angreifer und damit potentiell der Kontrolle über eine Vielzahl von virtuellen Maschinen. Hiermit ist das Thema der Verfügbarkeit unmittelbar verbunden, denn der Ausfall eines Host-Systems bedeutet nicht länger nur den Verlust eines Servers, sondern den Ausfall von x Servern in Form virtueller Maschinen. Dieses Risiko gilt es durch entsprechende Verfügbarkeitskonzepte (z.B. Verwendung von Clustern) zu minimieren, wobei speziell das Thema Cluster mit all seinen Facetten (Split-Brain-Syndrom, Fencing, Heartbeat, Cluster-fähige Dateisysteme etc.) nicht zur Vereinfachung des Gesamtsystems beiträgt.

Das Host-System (Hypervisor oder (Standard)-Betriebssystem plus Hypervisor, siehe Abbildung 2) wird damit zum Single Point of Failure. Neben einem direkten Angriff auf das Host-System kann ein Angriff auch anhand einer virtuellen Maschine erfolgen. Dass dies keine rein akademischen Risiken sind, wurde bereits mehrfach erfolgreich demonstriert (siehe (New) Blue Pill[2], SubVirt[3], etc.). Neben der vollständigen Kompromittierung sind aber auch partiell erfolgreiche Angriffe zu betrachten, z.B. Zugriff auf Arbeitsspeicher

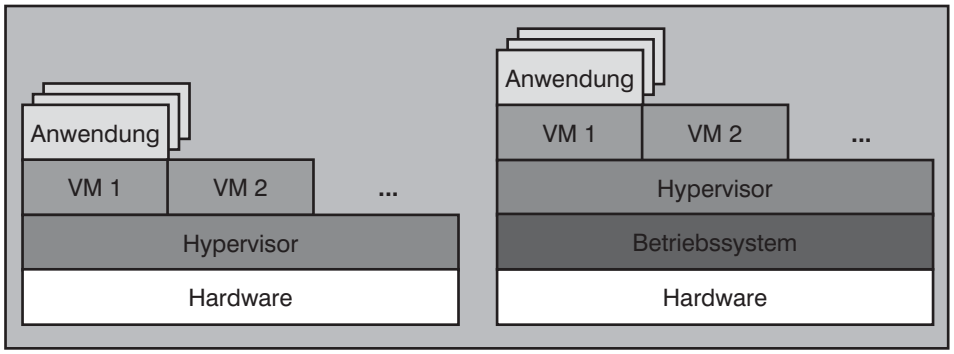


Abbildung 2: Hypervisor „Bare-Metal", Typ 1 (links) oder auf Basis eines Betriebssystems, Typ 2 (rechts)

[2]siehe http://bluepillproject.org/

[3]siehe http://www.eecs.umich.edu/virtual/papers/king06.pdf

oder Netzwerk, welches ein Ausspähen von sensiblen Daten ermöglicht, oder Angriffe vom Typ DoS (Zuweisung von mehr Ressourcen als vorgesehen, Blockade von bestimmten Funktionen wie Shutdown der virtuellen Maschine etc.). Auch wenn diese Risiken prinzipiell zu berücksichtigen sind, muss man sie dennoch relativieren. Bevor man sich explizit diesen technisch anspruchsvollen Angriffen widmet, sollte das Augenmerk auf Design und Implementierung nach „Best Practices“ und zugehörigem Management liegen. Dennoch existieren bereits Ansätze, diesen Angriffsvektor z.B. durch die Nutzung von TPM-Chips (Trusted Platform Module) zumindest zu erschweren.

Potentielle Risiken können bereits durch die Wahl der Virtualisierungsplattform verringert werden. Um die Angriffsfläche möglichst gering zu halten, empfiehlt sich generell ein Hypervisor, der direkt auf der Hardware („bare metal“) aufsetzt (Typ 1, Abbildung 2, links) und kein zusätzliches Betriebssystem als Plattform verwendet (Typ 2, Abbildung 2, rechts). Durch jede auf diese Weise eingesparte Zeile Quellcode wird nicht nur die Angriffsfläche verringert, sondern auch die Stabilität erhöht. Außerdem reduziert sich der Aufwand zur Absicherung, da für das Betriebssystem eines Typ-2-Hypervisors dedizierte Sicherheitsmaßnahmen (wie Härtung, Schutz vor schadenstiftender Software, etc.) umgesetzt werden müssen.

Beispiele für einen Typ-1-Hypervisor sind VMware ESXi („i“ für integrated) und Microsoft Hyper-V. Erwähnenswert ist dabei der Unterschied im Speicherplatzbedarf: während dieser bei VMware ESXi bei 32 MB liegt, kann Microsoft Hyper-V - auch bei Verwendung der Core-Server-Rolle - noch mind. 1 GB beanspruchen[4]. Produkte vom Typ 2, die ja auf Standardbetriebssystemen aufbauen, sind beispielsweise VMware Server oder Microsoft Virtual Server.

Für beide Virtualisierungsvarianten, sowohl Hypervisor vom Typ 1 als auch vom Typ 2, existieren zusätzliche Konfigurationsempfehlungen und Checklisten, welche die Sicherheit der Systeme erhöhen können. Ausgehend von den jeweiligen Unterlagen der Hersteller sowie einer Vielzahl von Online-Publikationen liefern speziell die Unterlagen des US-Verteidigungsministeriums (bzw. der Defense Information Systems Agency, kurz DISA) hilfreiche Informationen[5]. Aktuell besteht allerdings eine durchaus kontroverse Diskussion in der Virtualisierungsgemeinde über den Umfang und die Verantwortung des Herstellers der Virtualisierungslösung bzgl. der Sicherheit.

3.3 Sicherheit des Gastsystems

Das Host-System bzw. der Hypervisor stellt nur die Plattform für die produktiven Server bzw. Dienste dar. Neben den traditionellen Gefährdungen für physische Server, wie beispielsweise Viren und andere Programme mit Schadensfunktion, sind Gefährdungen zu berücksichtigen, die mit den Gastsystemen verbunden sind. Dies betrifft beispielsweise die Performance, wenn z.B. ein Fremdsystem unbeabsichtigt oder missbräuchlich Ressourcen-intensive Operationen durchführt. Hinzu kommt die Schnittstelle vom Gastsystem zum Hypervisor - zum einen in Richtung anderer virtueller Maschinen, zum anderen in Richtung des Host-Systems selbst. Dass diese Schnittstelle durchaus eine Gefährdung darstellt, zeigt ein Blick in das Verwundbarkeitsverzeichnis Common Vulnerabilities and Exposures (CVE)[6]: Hier werden für 2008 mindestens zehn solcher Schwachstellen in Produkten von VMware oder Xen aufgeführt[7].

In diesem Kontext findet sich auch der irreführenden Begriff „Rogue VM“ (analog zu „Rogue Access Points“), der besagt, dass virtuelle Maschinen unerwartet und ohne Genehmigung eingebunden werden können. Dies ist grundsätzlich falsch, da ohne Zugriff und explizite Konfiguration keine virtuelle Maschine in das Gesamtsystem eingebunden werden kann. Wahrscheinlicher sind menschliche Fehler (oder böswillige Absicht) durch an das Netz angebundene Systeme mit virtuellen Maschinen, die z.B. zu einem Rogue-DHCP-Server führen. Dies ist jedoch kein spezifisches Problem der Virtualisierung, auch wenn dies dadurch ggf. begünstigt wird und das Troubleshooting erschweren kann.

Um die Sicherheit der Gastsysteme zu gewährleisten, gelten vorwiegend die bereits bewährten Maßnahmenkataloge, welche beispielsweise die folgenden Punkte umfassen:

- Härtung des Betriebssystems
- Installation eines Anti-Virus-Programms
- Regelmäßige und zeitnahe Aktualisierung des Betriebssystems
- Beachtung der Sicherheitshinweise der jeweiligen Applikation
- Regelmäßige Sicherung des Systems einschließlich Übung der Wiederherstellung
- Monitoring, Dokumentation und Information über aktuelle Sicherheitslücken

Zusätzlich sind jedoch auch neue Maßnahmen zu berücksichtigen und bisherige ggf. neu zu bewerten. Dies beinhaltet z.B. die folgenden Maßnahmen:

- Entfernen nicht benötigter virtueller Hardware
- Aktualisierung der Virtualisierungs-Software innerhalb der virtuelle Maschine (z.B. VMware Tools)
- Isolation von Diensten, die bisher gemeinsam auf einer physischen Hardware liefen
- Regelmäßige und zeitnahe Aktualisierung der Applikationen

[4]siehe http://technet.microsoft.com/en-us/library/cc753802.aspx
[5]siehe http://iase.disa.mil/stigs/stig/index.html
[6]siehe http://cve.mitre.org/
[7]siehe auch Untersuchung zur Sicherheit in virtuellen Umgebungen: http://taviso.decsystem.g/virtsec.pdf

- Intensiveres Testen von Patches anhand der Virtualisierung einschließlich Wiederherstellung des vorherigen Zustandes (Snapshot- und Rollback-Funktion)

3.4 Sicherheit des virtuellen Netzes

Bezüglich der Sicherheit der Netzinfrastruktur muss berücksichtigt werden, dass in virtualisierten Systemen neben der Server-Landschaft auch die Vernetzung der Server virtualisiert wird. Für den internen Schutz solcher virtualisierten Netze stehen entsprechend virtualisierte Sicherheitselemente (wie z.B. IDS/IPS oder Firewall) zur Verfügung.

Bezüglich der Funktionsweise virtueller Switche, möglicher Topologien im Zusammenspiel zwischen virtuellen und physischen Netzelementen und der Isolation unterschiedlicher Sicherheitszonen wurde bereits detailliert im Netzwerk Insider vom November 2008 eingegangen, auf den an dieser Stelle verwiesen wird[8]. Abbildung 3 illustriert den Aufbau virtueller Sicherheitszonen, d.h. virtuelle Netze, die durch virtualisierte Sicherheitselemente geschützt werden.

Die Komplexität der Konfiguration virtueller Netze dürfte damit in Zukunft der physischen Infrastruktur in nichts nachstehen. Aktuell müssen virtualisierte Sicherheitsprodukte (wie sie derzeit von einigen Herstellern forciert werden) außerdem noch skeptisch betrachtet werden. Diese stellen derzeit in der Regel keinen Ersatz für physische Komponenten dar, sondern können ggf. als Ergänzung betrachtet werden. Dies hat zunächst zwei Gründe:

- Performance: Insbesondere Anforderungen im Gigabit-Bereich, für die bisher spezielle Hardware zum Einsatz kam, können aktuell nicht durch virtualisierte Sicherheitsprodukte realisiert werden. Beispielsweise haben Produkte im Bereich Unified Threat Management (UTM), die neben Firewall-Funktion weitere CPU-intensive Aufgaben wie Pattern-Analysen, Viren-Überprüfungen bündeln, erhebliche Leistungsanforderungen.

- Sicherheit: Diese Produkte sind neu und damit bisher wenig erprobt. Ihre Zuverlässigkeit müssen sie daher noch unter Beweis stellen. Weiterhin handelt es sich um normale virtuelle Maschinen. Somit gelten für sie die gleichen Gefährdungen wie für andere virtuelle Gastsysteme bzw. die gesamte virtuelle Infrastruktur.

Besonders kritisch für die sichere Vernetzung von virtuellen Servern ist jedoch die im Folgenden beschriebene Dynamik und Mobilität der Systeme.

3.5 Besondere Berücksichtigung der Dynamik und Mobilität

In der traditionellen Server-Nutzung ist die Zuordnung von Sicherheitsmaßnahmen zu einem Server meist eher statisch. Der Server wird konfiguriert und verrichtet für einen längeren Zeitraum seinen Dienst. Das Bündel von Sicherheitsmaßnahmen, das auf den Server und die dort laufenden Anwendungen angewendet wird, muss nur bei gravierenden Änderungen des Systems (also meist selten) angepasst werden.

Bei Nutzung virtueller Server ist dies jedoch ein hochgradig dynamischer Prozess!

Der Aufenthaltsort eines Servers ist in einer virtuellen Umgebung nicht länger statisch. Das Aufsetzen eines virtuellen Servers reduziert sich umgangssprachlich auf einen Doppelklick. Der virtuelle Server kann dann mit entsprechenden Bordmitteln der Virtualisierungslösung (z.B. VMware VMotion, Citrix oder Microsoft Live Migration) sogar ohne Unterbrechung des laufenden Betriebs auf einen anderen physischen Server migriert werden. Dieses Verschieben von virtuellen Maschinen zwischen verschiedenen Host-Systemen im laufenden Betrieb (nur Arbeitsspeicher oder auch Festplattendateien) kann beispielsweise aufgrund eines Ausfalls oder einer Ressourcenoptimierung erfolgen.

In bisherigen physischen Infrastrukturen sind Sicherheitsarchitekturen hochgradig von physischen Gegebenheiten abhängig, wie z.B. Switches, NICs oder anderen Sicherheitselementen. Eine virtualisierte Umgebung erfordert, dass dieser Sicherheitskontext dynamisch auf allen potentiellen Host-Systemen zur Verfügung steht und dabei die Abhängigkeiten zu anderen Systemen berücksichtigt werden.

In der Konsequenz bedeutet dies:

- Speicherinhalte und ggf. auch der gesamte Server samt Massenspeicher (Beispiel: VMware Storage VMotion) müssen über das Netz transportiert werden.

  In der Standardkonfiguration erfolgt dieser Transport oft im Klartext. Je nach Schutzbedarf der transportierten Daten müssen also Sicherheitsmaßnahmen

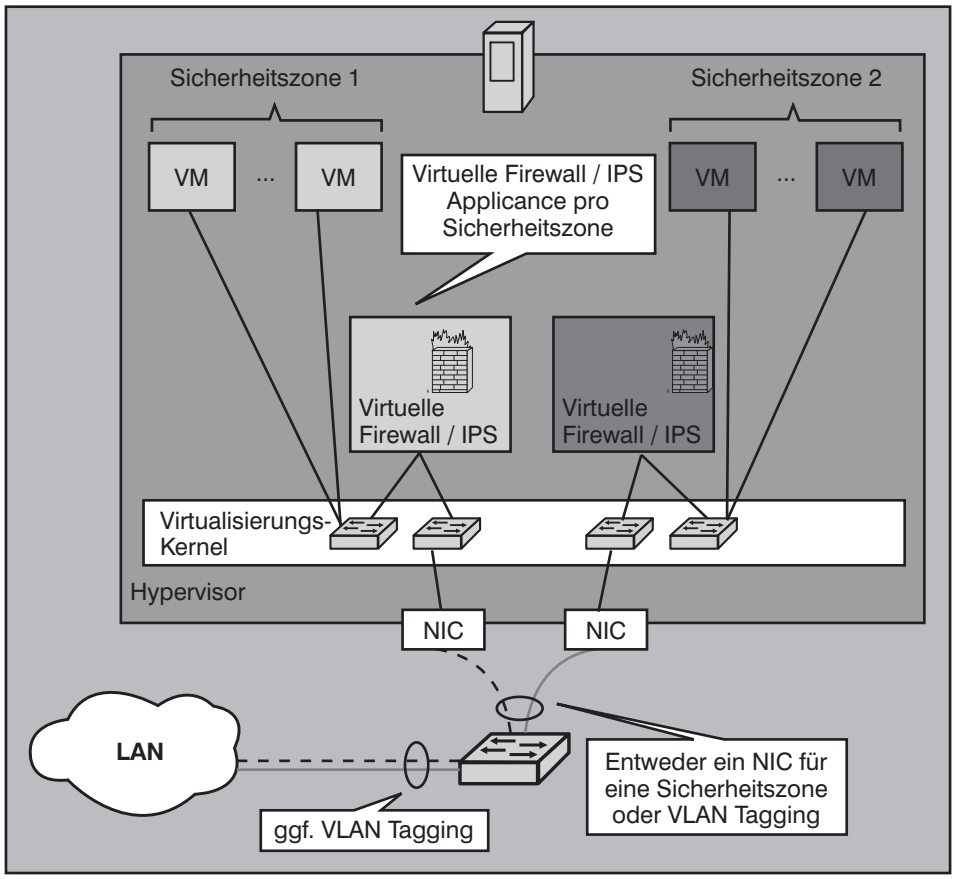


Abbildung 3: Virtualisierung von Sicherheitszonen

[8]siehe http://www.comconsult.com/papers/Sicherheitszonen-in-LAN-und-Rechenzentrum.pdf

umgesetzt werden. Zu nennen sind hier die zusätzliche Verschlüsselung des Netzverkehrs (z.B. per IPsec) oder zumindest die Nutzung eines separaten physischen Netzes bzw. VLAN für das Verschieben virtueller Server zwischen physischen Servern.

- Der Sicherheitskontext muss am Quell- und Zielort identisch sein.

  Dabei muss neben den auf den physischen Server angewendeten Sicherheitsmaßnahmen insbesondere die virtualisierte Netzumgebung des virtuellen Servers berücksichtigt werden. Dies beinhaltet beispielsweise zunächst Konfiguration und Regelwerk einer virtualisierten Firewall. Wenn ein Server im laufenden Betrieb umgezogen wird, muss neben dem Zustand des Servers auch der komplette für den Server relevante Zustand einer entsprechenden Firewall umziehen (etwa Informationen, welche Sitzungen aktuell bestehen). Analog müssen Switch-Konfigurationen (z.B. VLANs, QoS-Parameter, etc.) übertragen werden und Aspekte des Monitorings (z.B. Traffic-Verbrauch, der anhand flüchtiger Zählerwerte festgehalten wird) berücksichtigt werden.

Cisco adressiert dieses Thema Server-übergreifender Netzkomponenten und damit auch Sicherheitskontexte aktuell beispielsweise mit dem Nexus 1000V.

VMware hat mit vShield Zones jetzt ein Konzept vorgestellt, das die Umsetzung von Sicherheitsvorgaben für die virtuellen Maschinen auch dann sicherstellen soll, wenn einzelne virtuelle Server zwischen physischen Servern migriert werden. Im Frühjahr 2009 soll hierzu ein Betaprojekt starten.

Es ist weiterhin zu erwarten, dass auch andere Hersteller in diesem Bereich Produkte auf den Markt bringen werden und neben der Thematik dynamischer Sicherheits- und Netzkontexte auch folgende Bereiche abdecken:

- Management (Skalierbarkeit, Integration in physische Netzinfrastruktur, etc.)
- Monitoring (z.B. via SNMP oder Netflow)
- Funktionsumfang (QoS, AAA, ACLs, etc.)

3.6 Sicherheit der Datenspeicher und des Speichernetzes

Ein virtueller Server (bzw. der Massenspeicher eines virtuellen Servers) besteht in der Regel nur noch aus einzelnen Dateien. Diese können bei ungenügender Absicherung z.B. auf mobile USB-Datenträger kopiert werden. Der Angreifer verfügt damit über ein vollständiges Abbild des Servers, das er offline analysieren kann. Dieses Abbild muss der Angreifer nicht zwangsläufig booten und weitere Sicherheitsmaßnahmen, wie z.B. Bootloader-Passwort oder Betriebssystem-Login überwinden, um an die Daten zu gelangen. Stattdessen kann er unter Umständen das Image direkt in die Verzeichnisstruktur (z.B. als zusätzlichen Laufwerksbuchstaben) einbinden und erhält auf diese Weise Zugriff auf die Daten.

Bei der Verwendung eines Speichernetzes (SAN) ergeben sich zudem folgende Risiken:

- Auf IP-basierte Speichersysteme (z.B. iSCSI) vererben sich zunächst automatisch alle Gefährdungen von IP.
- Daten der virtuellen Maschinen (z.B. der Inhalt des Arbeitsspeichers) bzw. vollständige virtuelle Server werden i.d.R. unverschlüsselt über das Netz transportiert. Vertraulichkeit sowie Daten- und Hostintegrität sind also gefährdet. Im Fall von IP-basierten Speichersystemen sind Übertragungswege und Netzkomponenten nicht zwingend reserviert für Speicherverkehr, sondern werden von verschiedensten anderen Verkehrstypen gemeinsam genutzt.
- Anhand von Manipulationen kann ein Zugriff auf nicht erlaubte Datenpartitionen erfolgen (z.B. Daten anderer Sicherheitszonen).

Der letzte Punkt ist eine mögliche Konsequenz, wenn Speicherplatz als zentrale Ressource Systemen unterschiedlicher Sicherheitszonen zugewiesen wird. Ein gesondertes SAN für eine DMZ oder verschiedene Fachabteilungen ist zumindest nicht die Regel. Wird beispielsweise ein solcher Server der DMZ kompromittiert, besteht die Gefahr, dass dieser Server Zugriff auf Datenpartitionen erhält (z.B. mittels IQN/WWN Spoofing), die eigentlich einem Server z.B. der Personalabteilung vorbehalten sind. Diese Gefährdung besteht zunächst generell, sie wird jedoch durch virtuelle Server deutlich erhöht.

Zu den möglichen Maßnahmen gehören:

- Aufbau eines zumindest logisch getrennten dedizierten Netzes für Speicheranbindung und Management
- Berücksichtigung von Zonierungen innerhalb des Speichernetzes (SAN Zoning, Virtuelle SANs, etc.), so dass entsprechende Sicherheitszonen gebildet werden können
- Authentisierung zwischen Client und Server (z.B. beidseitiges CHAP bzw. DH-CHAP)
- Verschlüsselung auf Ebene des Netzes (z.B. per IPsec oder IEEE 802.1AE) oder sogar Verschlüsselung auf Ebene des Speichermediums

4. IT-Sicherheitsmanagement und Virtualisierung

Die beschriebenen technischen Aspekte der Absicherung virtueller Server haben unmittelbare Konsequenzen für das IT-Sicherheitsmanagement und die Gestaltung von Sicherheitskonzepten.

Zunächst muss, wie bereits erwähnt, die Server-Virtualisierung in den Sicherheitskonzepten Server, Betriebssysteme und Anwendungen berücksichtigt werden (Abbildung 4). Die in diesem Artikel beschriebene Komplexität legt die Erstellung eines eigenständigen Sicherheitskonzepts mit einem spezifischen Maßnahmenkatalog für den Umgang mit Server-Virtualisierung nahe.

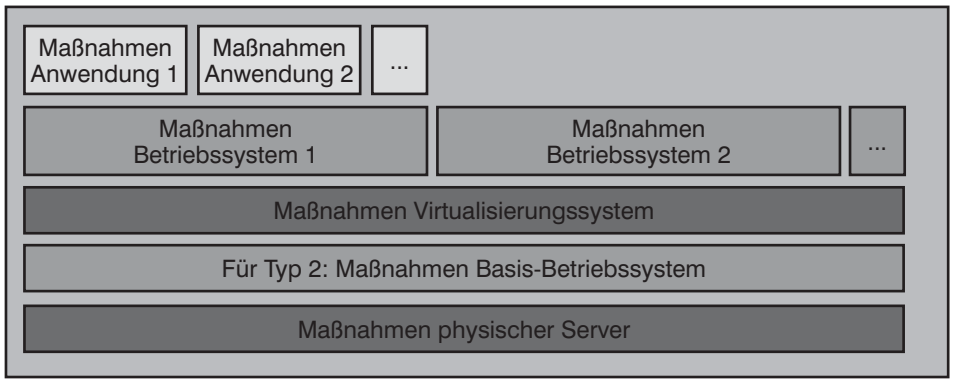


Abbildung 4: Berücksichtigung der Server-Virtualisierung in Sicherheitskonzepten

Insbesondere müssen Datensicherungskonzepte und Notfallvorsorgekonzepte für den Umgang mit Server-Virtualisierung angepasst werden. Außerdem steigen meist durch einen Kumulationseffekt die Sicherheitsanforderungen an die physischen Server. Auch hier müssen die bestehenden Sicherheitskonzepte und Betriebsprozesse ggf. entsprechend erweitert werden, bzw. es wird die Anzahl der virtuellen Server pro physischem Server begrenzt (und zur Vorgabe für den Durchschnittsfall erklärt), bis zu der ein möglicher Kumulationseffekt nicht berücksichtigt werden braucht.

Die Flexibilität und Dynamik der Server-Virtualisierung hat unmittelbare Auswirkungen auf die Vorgehensweise bei der Feststellung des Schutzbedarfs und der Auswahl der auf ein IT-System anzuwendenden Sicherheitsmaßnahmen.

Grundlage einer praktikablen sicheren Server-Virtualisierung ist dabei die Normierung von virtuellen Servern. Dies beinhaltet zunächst Konfigurationsvorgaben an das Betriebssystem auf den virtuellen Servern sowie die Festlegung der Anwendungsbereiche und der Dienste. Unabhängig von dem für die konkreten virtuellen Server bestimmten Schutzbedarf (beispielsweise unter Verwendung der BSI-Methodik) wird von vorneherein festgelegt, dass als Ausgangspunkt nur einer der normierten virtuellen Server herangezogen werden darf. Dieser kann bei Bedarf noch gezielt weiter abgesichert werden. Andere Formen der Diversifizierung von Sicherheitskonfigurationen für virtuelle Server werden nicht zugelassen.

Wer diese Strategie zur sicheren Grundkonfiguration von virtuellen IT-Systemen verlässt, handelt sich unweigerlich eine unüberschaubare Sammlung aus Einzellösungen ein, die schon bei dedizierten Servern nicht zu empfehlen ist. Im Fall virtueller Systeme mit der Addition von zu härtender Virtualisierungsbasis (Hard- und Software) und zu härtenden virtuellen Maschinen entstünde eine Matrix aus möglichen Kombinationen, die sicherheitstechnisch nicht mehr mit verhältnismäßigem Aufwand bewertbar und aktualisierbar ist (Patch-Management, Change Management unter Aufrechterhaltung des erforderlichen Sicherheitsniveaus).

Für jeden auf die beschriebene Weise normierten virtuellen Server kann ein Maßnahmenbündel spezifiziert werden, indem beispielsweise die anwendbaren Maßnahmen der entsprechenden Bausteine der BSI IT-Grundschutzkataloge ausgewählt werden. Dabei kann im Rahmen der Normierung sofort ein Maßnahmenbündel für den normalen Schutzbedarf (Mindesthärtung) sowie ein hierauf aufbauendes erweitertes Maßnahmenbündel für den erhöhten Schutzbedarf (Basishärtung für erhöhten Schutzbedarf) festgelegt werden. Die wesentlichen Vorgaben können dann als Konfigurationsrichtlinie für jedes Gastbetriebssystem festgelegt werden.

Werden die so geschaffenen Umgebungsstandards für normierte virtuelle Server der Varianten „Schutzbedarf normal“ bzw. „Schutzbedarf erhöht“ in geeigneter Form verwaltet und bei der Serverimplementierung vervielfältigt, tut eine gelegentliche „Übererfüllung“ der Sicherheitsanforderungen bei Einsatz eines Profils für den erhöhten Schutzbedarf aufwandstechnisch nicht weh. Einrichtungsaufwand ist auf diese Weise kein Gegenargument gegen normierte virtuelle Server zur Optimierung der Effizienz im Sicherheitsmanagement. Für die praktische Umsetzung bietet die Virtualisierung hierzu mittels entsprechender „VM-Bibliotheken“ eine einfache Möglichkeit virtuelle Server auf Basis obiger Konfigurationsrichtlinien zu hinterlegen und bei Bedarf zu klonen, um eine höchstmögliche Übereinstimmung mit den Konfigurationsrichtlinien zu erzielen.

Anschließend können Vorgaben für die Abbildung der normierten virtuellen Server auf den physischen Servern gemacht werden. Hier muss beispielsweise festgelegt werden, ob man virtuelle Server, die unterschiedlichen Vertrauensbereichen zuzu-

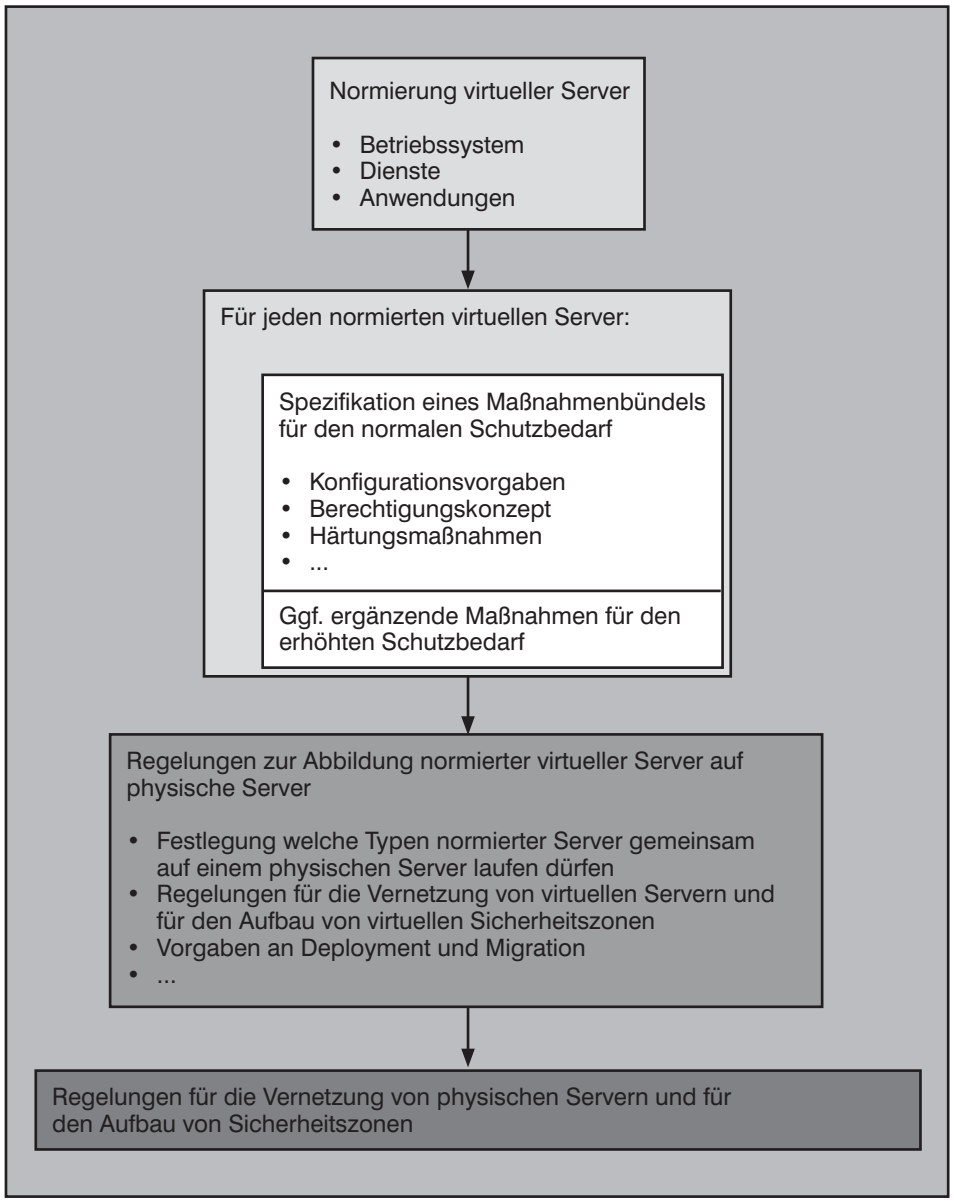


Abbildung 5: Strukturierte Vorgehensweise bei der Absicherung virtueller Server-Umgebungen

ordnen sind, auf einem physischen Server laufen lassen darf oder nicht. Auf dieser Basis können dann die (virtuelle) Vernetzung der normierten virtuellen Server spezifiziert und Regelungen für die Migration zwischen verschiedenen physischen Systemen erarbeitet werden. Dies beinhaltet neben Maßnahmen für die Konfiguration der virtuellen Switches (z.B. kein Promiscuous Mode auf virtuellen Switches) ggf. auch die Gestaltung virtueller Sicherheitszonen verbunden mit Vorgaben an das Regelwerk virtualisierter Firewalls.

Insgesamt ist für jeden physischen Server festzulegen, welche virtuellen Server bzw. Typen von virtuellen Maschinen auf ihm laufen dürfen. Der Schutzbedarf der physischen Server ergibt sich dann durch Vererbung des Schutzbedarfs der einzelnen virtuellen Systeme unter Berücksichtigung eines Kumulationseffekts. Dieser Kumulationseffekt kann – auch wenn die einzelnen virtuellen Systeme nur einen normalen Schutzbedarf haben – einen erhöhten Schutzbedarf eines physischen Servers bedingen, weil sich das Gefährdungspotential mit der Anzahl der virtuellen Systeme entsprechend erhöht. Abbildung 5 zeigt die beschriebene Vorgehensweise im Überblick.

Im Rahmen der Ergänzung und Überarbeitung der Sicherheitskonzepte sollte auch geprüft werden, ob allgemeine Policies durch den Einsatz von Virtualisierung betroffen sind. Ein Beispiel in diesem Zusammenhang sind Compliance-Anforderungen, wie sie für Kreditkarten-verarbeitende Unternehmen in Form des Regelwerks PCI DSS (Payment Card Industry Data Security Standard) relevant sind. Hier ist unter anderem der Punkt 2.2.1 im Zusammenhang mit der Virtualisierung von Interesse. Dieser besagt: „Implementieren nur einer primären Funktion pro Server.“ Je nach Auditor gab es in diesem Zusammenhang bisher Unklarheiten, wie dies in einer virtuellen Umgebung zu betrachten ist, da hier mehrere Funktionen auf einem physischen Server untergebracht sind, die Funktionen dennoch isoliert in virtuellen Maschinen ablaufen können. Um in diesem Punkt Abhilfe zu schaffen, ist z.B. VMware der PCI-Gruppe im November 2008 beigetreten. In Zukunft wird das Thema Virtualisierung also auch hier konkrete Berücksichtigung finden.

5. Fazit

Die Server-Virtualisierung lässt sich nicht auf eine reine Serverkonsolidierung reduzieren. Es handelt sich vielmehr um eine neue Architektur mit Auswirkungen auf den gesamten IT-Verbund, angefangen beim IT-Sicherheitsprozess über die Umgestaltung von IT-Sicherheitskonzepten bis hin zur Umsetzung entsprechender Maßnahmen.

Dabei liegt die Herausforderung in der Beherrschbarkeit der abstrahierten IT-Infrastruktur und weniger in Gefährdungen durch ausgefeilte, besonders für die Virtualisierungstechnik erdachte Angriffe. Zur Notwendigkeit, sich mit einer neuen Generation von Produktlösungen für den Serverbereich zu beschäftigen, kommt die Problematik, dass bislang über eigenständige Geräte unterscheidbare Teile der IT-Infrastruktur in einem Gesamtsystem verschmelzen. Die Übersicht geht leichter verloren, und die Kontrolle auf Funktionieren der Kommunikation und Zuständen der Server muss neu gelernt werden. Kombiniert sich dies mit einer Vielzahl an Konfigurationsalternativen, so steht man leicht vor einem sicherheitstechnisch unkontrollierbaren Gebilde. Abhilfe schaffen hier festgelegte (Umgebungs-)Standards und Prozesse sowie ein hoher Automatisierungsgrad bei der Nutzung entsprechender Werkzeuge. Kritisch sind die Seiteneffekte, die sich aus der Dynamik und Mobilität der virtuellen Server ergeben. Hier werden höchste Anforderungen an das Configuration Management und das Release Management mit unmittelbaren Auswirkungen auf die IT-Sicherheit gestellt. Ohne konsequente Standardisierung in Aufbau, Deployment, Vernetzung und Migration virtueller Server droht ein deutlicher Verlust an Sicherheit.

6. Abkürzungen

AAA	Authentication, Authorization, Accounting
ACL	Access Control List
CHAP	Challenge Handshake Authentication Protocol
CPU	Central Processing Unit
CVE	Common Vulnerabilities and Exposures
DH-CHAP	Diffie Hellman - Challenge Handshake Authentication Protocol
DISA	Defense Information Systems Agency
DMZ	Demilitarized Zone, Demilitarisierte Zone
DoS	Denial of Service
HBA	Host Bus Adapter
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
IQN	iSCSI Qualified Name
iSCSI	internet Small Computer System Interface
LAN	Local Area Network
NIC	Network Interface Card
QoS	Quality of Service
SAN	Storage Area Network
SNMP	Simple Network Management Protocol
TPM	Trusted Platform Module
UTM	Unified Threat Management
VLAN	Virtual LAN
VM	Virtual Machine, Virtuelle Maschine
WWN	World Wide Name

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Trouble Shooting für Netzwerk-Anwendungen, 17.03.-20.03.09 in Aachen

Dieses Seminar beschreibt die typischen Störsituationen im Umfeld moderner Anwendungen, gibt Einblick in bisher als Black Box benutzte Mechanismen und Abläufe und trainiert die systematische und methodische Diagnose und Fehlerbeseitigung. Dabei wird die Theorie mit praktischen Übungen und vielen Fallbeispielen in einem Trainings-Netzwerk kombiniert. Die Teilnehmer werden durch dieses kombinierte Training in die Lage versetzt, das Gelernte sofort in der Praxis umzusetzen. Als Protokoll-Analysator kommt Wireshark zum Einsatz. Einer Verwendung selbst mitgebrachter Analyse-Software, mit deren Bedienung der Teilnehmer vertraut ist, steht nichts im Wege.

Preis: € 2.190,- zzgl. MwSt.

Office Communications Server 2007, 30.03. - 31.03.09 in Köln

In diesem Seminar werden sowohl die technischen als auch die strategischen Aspekte des Office Communications Servers analysiert. Unsere herstellerunabhängigen und neutralen Experten haben sich sehr ausführlich mit den technischen Details befasst und verfügen über langjährige Erfahrung bei der Implementierung von Microsoft-Lösungen, bei der Konzeption von TK-Lösungen sowie bei der Bewertung von Kommunikationstechnologien.

Preis: € 1.390,- zzgl. MwSt.

Sicherheit 2: Erarbeitung und Umsetzung von Sicherheitskonzepten, 30.03. - 03.04.09 in Berlin

Sicherheitskonzepte müssen mehr sein als Papier. Ihre erfolgreiche Umsetzung erfordert: eine umsichtige Planung und Beschaffung der Sicherheitsinfrastruktur, eine effektive Integration in Prozesse und Organisation, konzeptkonforme Einbindung externer Leistungen (Lieferung, Implementierung, Wartung und Betriebsleistungen). Bei der notwendigen Erfolgskontrolle helfen Standards wie BS7799, ISO 27001 und die IT-Grundschutz-Standards und -Kataloge des BSI. Eine entsprechende Zertifizierung des erreichten Sicherheitsniveaus ist möglich, aber auch eine Verwendung solcher Standards als internes Hilfsmittel.

Preis: € 2.290,- zzgl. MwSt.

Projektmanagement II: Sitzungen moderieren, Projekte präsentieren, erfolgreich verhandeln und Projektteams leiten, 30.03. - 03.04.09 in Berlin

In diesem 5-tägigen Intensiv-Seminar steht das Führungsverhalten des Projektleiters eindeutig im Mittelpunkt. Professionelles Moderieren, Präsentieren, Verhandeln und Teamleiten ist eine Kunst, die trainierbar ist. Anhand begleitender Rollenspiele und Praxisübungen werden die führungsrelevanten Eigenschaften klar verbessert.

Preis: € 2.290,- zzgl. MwSt.

SIP (Session Initiation Protocol)- Basis-Technologie der IP-Telefonie, 30.03. - 01.04.09 in Berlin

Dieses 3-tägige Seminar vermittelt Planern und Betreibern Anforderungen und Technologien für den Einsatz von Telefonie und Mehrwertdiensten auf Basis des neuen Standards SIP. Chancen und Risiken werden anhand von Einsatzszenarien bewertet und kontrovers diskutiert.

Preis: € 1.690,- zzgl. MwSt.

Ethernet-Netzwerke: Techniken, Einsatzgebiete und Betrieb, 20.04. - 22.04.09 in Aachen

Dieses Seminar stellt die aktuellen Ethernet-Themen vor und zeigt, wie etablierte und neue Techniken in bereits wohlbekannten und zukünftigen Anwendungsgebieten eingesetzt werden können. Zu den analysierten Sonderanwendungsgebieten gehören insbesondere VoIP, Gefahrenmeldetechniken, Industrienetze und Rechenzentrumsbereiche. Mit besonderem Blick auf die Praxis werden Komponenten- und Kabeltechnik erläutert, Planungsregeln vorgestellt, Möglichkeiten und Grenzen von Quality of Service und Risiken durch Fehlentscheidungen bei der Technikauswahl aufgezeigt. Aufbau von Infrastrukturen, Fehlersuche und das allgegenwärtige Thema Sicherheit werden aus der Praxis moderner Ethernet-Netze beleuchtet.

Preis: € 1.690,- zzgl. MwSt.

Projekt-Erfahrungsbericht: Cisco CallManager Rollout und Migration CUCM Version 6, 27.04. - 28.04.09 in Aachen

Dieses Seminar bietet sowohl Projektleitern, als auch Administratoren einen einmaligen Überblick über die Problemfelder, Fragenstellungen und Chancen bei der Planung, Einführung und dem Betrieb einer Unified Communications-Lösung. Es zeigt, dass die Einführung von IP-Telefonie nicht nur technische Problemstellungen aufwirft, sondern auch organisatorische Antworten erforderlich macht. Diese wiederum haben deutliche Auswirkungen auf die Konfiguration und die Installation der Lösung, so dass sich hier der Kreis schließt.

Preis: € 1.390,- zzgl. MwSt.

Elektrische Störungen in Datennetzen und Computerinstallationen erfolgreich erkennen und beseitigen, 28.04. - 29.04.09 in Bonn

Sie erfahren in diesem 2-tägigen Seminar, welche typischen Ursachen den in den letzten Jahren festgestellten Störungen und Schäden in Netzwerken und DV-Installationen zu Grunde liegen, wie gefährlich diese Störungen sind und wie sie messtechnisch erkannt und beseitigt werden können.

Preis: € 1.390,- zzgl. MwSt.

IP-Wissen für TK-Mitarbeiter, 04.05. - 05.05.09 in Königswinter

Dieses Seminar vermittelt kompakt und effizient das IP-Wissen, das TK-Mitarbeiter ohne Vorkenntnisse zur Planung und zum Betrieb von IP-basierten Telefonie-Lösungen benötigen.

Preis: € 1.390,- 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
05.05. - 08.05.09 in Aachen
06.10. - 09.10.09 in Aachen

Trouble Shooting 2
17.03. - 20.03.09 in Aachen
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
30.03. - 03.04.09 in Berlin
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
30.03. - 01.04.09 in Berlin
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 evaluieren, planen, betreiben
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
04.05. - 05.05.09 in Königswinter
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