

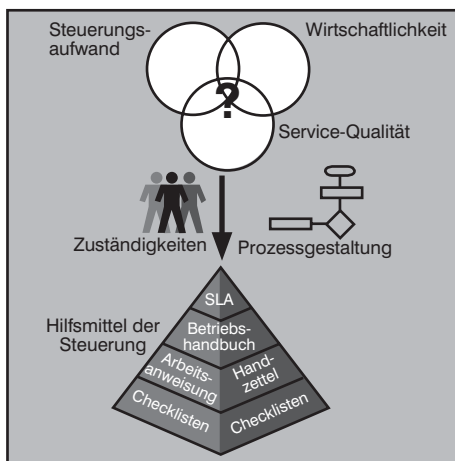
## Schwerpunktthema

## Service Level - Steuerung der Leistungsqualität in der Praxis

von Dipl.-Inform. Oliver Flüs

### 1. Situation

Entsprechend der Wichtigkeit, die IT heutzutage praktisch überall bekommen hat, werden auch Begriffe wie „Dienstleistung“, „Qualität“ u.ä. im Zusammenhang mit Aufgaben der Bereitstellung von IT immer selbstverständlicher. Früher als Zwischending zwischen Technik-Guru und Hausmeister für besondere stromkonsumierende Lösungen gehandelt, ist ein IT-Betreiber heute ein „Manager“, der eine Service-Leistung anbietet. Auch scheint die Phase vorüber, in der jeder Anwender potenziell ein bisschen IT-Spezialist war und sich im Zweifel mit Tricks und Selbsthilfe über Kinderkrankheiten der Lösungen hinweghelfen musste.



Die Technik hat eine durchaus gute Grundstabilität erreicht - Trouble Shooting konzentriert sich mit wachsendem Anteil auf Aspekte von Minderperformance oder Probleme, die durch „Zweckentfremdung“ entstehen: Lösungen werden für Zwecke verwendet, für die sie nicht konzipiert waren, so dass hierdurch besondere Schwierigkeiten entstehen.

weiter auf Seite 15

## Zweitthema

## Notfallvorsorge für IT - flexibel und bedarfsgerecht

von Dipl.-Inform. Oliver Flüs

### 1. Notfallvorsorge allgemein - was kann man davon lernen?

Für den Notfall vorsorgen- dies ist ein Thema, das man in letzter Zeit mehrfach als durchaus wichtig vor Augen geführt bekam. Wassereinbrüche, Hochwasser oder sogar Tsunami einerseits und die Bedrohung durch stark ansteckende Krankheiten wie Grippe oder Masern (jüngst erst wieder in NRW) andererseits, es gibt ge-

nügend Auslöser von echten Ausnahme-situationen, die nicht einfach durch „Warten bis es vorbei ist“ überbrückt werden können.

Die Notwendigkeiten einer gezielten Vorbereitung auf den Notfall betreffen sämtliche Aspekte und Ausstattung, die eine Unternehmung zur Gewährleistung ihrer Handlungsfähigkeit braucht. Die IT-Ausstattung ist damit natürlich sofort mit im

Fokus der Aufgabenstellung, gibt es doch praktisch niemanden mehr, der ernsthaft behaupten würde, er sei ohne Rückgriff auf IT-Ausstattung vollständig oder auch nur annähernd im normalen Umfang arbeitsfähig.

weiter Seite 7

## Top Veranstaltung

### Voice-over-IP-Forum 2006

auf Seite 5

## Zum Geleit

### IP-Telefonie: die nächste Generation steht vor der Tür, Cisco und Siemens in der Sackgasse?

auf Seite 2

## Report des Monats

### VPN-Technologien: Alternativen und Bausteine einer erfolgreichen Lösung

auf Seite 13

Zum Geleit

# IP-Telefonie: die nächste Generation steht vor der Tür, Cisco und Siemens in der Sackgasse?

Unsere laufenden Analysen zur weiteren Marktentwicklung im Voice-Markt haben die nachfolgende in Teilen durchaus drastische Markteinschätzung ergeben. **Wir sind an Ihrer Meinung dazu interessiert und suchen Ihre Rückmeldung**, siehe dazu am Ende mehr!

In den letzten Jahren dominierte die Frage der Ablösung der traditionellen Telefonie durch IP-Telefonie den Markt. Funktionsmerkmale wurden fleißig verglichen, Betriebskosten hin und zurück gerechnet. Nun, da jedem klar ist, dass die traditionelle Telefonie im Neugeschäft die nächsten 3 Jahre nicht überleben wird, kommen selbst die härtesten Traditionalisten nicht umhin, die neue Technik zu akzeptieren (die installierte Basis wird sicher noch deutlich länger im Markt bleiben).

Mit dieser Erkenntnis und den sich verziehenden Pulverschwadern ist aber auch die große Leere gekommen. Ging es bei der ganzen Auseinandersetzung nur um die Frage, einen Hörer abzuheben und mit einer anderen Person zu sprechen? Ist das so revolutionär, dass wahre Glaubenskriege ausgetragen werden müssen? Ist die Einstufung als höchst strategisches Thema für ein Unternehmen damit überhaupt gerechtfertigt? Parallel hat auch die Normalisierung der Technik durch Anbieter wie Skype der IP-Telefonie den Glorienschein geraubt. Was ist eigentlich so toll und teuer an einer Technologie, die mit einem kleinen und einfachen Programm auf jedem PC und Mac kostenfrei installiert werden kann? Das ist zugegeben übersimplifiziert und leicht polemisch, hat aber einen wahren Kern. Die ganze technische Situation der Vergangenheit basiert auf komplexen, hardwaretechnischen Hersteller-Lösungen. In dem Moment, in dem ein Übergang zu softwarebasierten Standards erfolgt, ist das die Nadel im Luftballon. Genau aus diesem Grund wird der Trend zur Normalität, zur elementaren Basistechnologie durch den SIP-Standard weiter verstärkt. Telefonie-Grundfunktionalität (wir wollen jetzt keine Diskussion über 500 Leistungsmerkmale führen) wird in sehr kurzer Zeit einfach da sein. Und wirklich Niemand mehr wird gewillt sein, dafür zu bezahlen. Diese Grundfunktionalität wird auch in 3 bis 5 Jahren keine Magerfunk-



tionalität mehr sein, der Funktionsumfang wird nach unserer Einschätzung (Investitions-)kostenfrei zu 90% dem Umfang einer traditionellen TK-Lösung entsprechen.

Damit steht auch das traditionelle Geschäftsmodell des Telefonie-Enterprise-Markts auf dem Prüfstand. Die Erkenntnis ist so simpel wie weit reichend: das alte Geschäftsmodell ist tot, auf seiner Basis kann ein Unternehmen kein Geld mehr verdienen. Dementsprechend leben die traditionellen Anbieter zwar noch von ihrer weit reichenden installierten Basis, aber die Endlichkeit dieser Lebensader ist offensichtlich. Die Diskussionen um den Enterprise-Com-Bereich von Siemens sind ein typisches Beispiel für diese Übergangsphase.

Aber auch die Angreifer aus der Daten und Netzwerk-Welt stehen immer mehr vor der Frage, ob sie den Kampf nun wirklich gewonnen haben. Zwar überschlagen sie sich fast täglich mit Ankündigungen neuer Rekorde verkaufter Telefone, doch unter dem Strich muss auch ihr Geschäftsmodell angesichts der zunehmenden kostenfreien Normalität in Frage gestellt werden. Im Endeffekt ist jedem Beteiligten klar, dass Geld nur mit einer weitergehenden auf Sprache aufsetzenden Zusatz-Funktionalität verdient werden kann.

Auf diese Herausforderung reagieren die Anbieter zur Zeit. Herausragend sicher der Schwenk von Cisco mit der Ankündigung des Call-Manager 5 zur CeBit. Hier wird

technisch mit nahezu allem gebrochen, was Cisco bisher für heilig erklärt hatte. Und mit diesem Schritt wird der Weg in die Betonung von neuen Funktionen und der Orientierung an Geschäftsprozessen geöffnet. Betrachtet man die letzten öffentlichen Auftritte von John Chambers, dann ist von den klassischen Telefonie-Funktionen keine Rede mehr. Prozess-Optimierung, Kollaboration und Präsenz stehen im Vordergrund. Dumm nur, dass die dabei herausgestellten Funktionen, die nach Chambers Darstellung unverzichtbar sind, im Call Manager 4 nicht enthalten sind. Der Wechsel in eine neue Produktstrategie kostet Zeit, voraussichtlich 1 bis 2 Jahre. In dieser Übergangszeit wird der Kunde vor dem Problem stehen, dass der neuen Welt wesentliche Funktionen der alten Welt fehlen, die alte Welt aber den eigentlichen Kern zukünftiger Kommunikation nicht abbildet. Was nun? Nun für Cisco-Kunden wird erst 5.2 den Frieden wieder herstellen. Bis dahin hängt die Entscheidung von wichtigen technischen Details ab, die man unbedingt kennen muss.

Auch bei Siemens sieht die Situation nicht anders aus. Die HiPath 8000 macht noch keinen wirklich reifen Eindruck, die HiPath 4000 hat ohne Zweifel den Geruch fehlender Zukunftsorientierung. Um das Ganze abzurunden, hat Siemens wichtige neue Funktionalitäten auf OpenScape konzentriert und nicht in seine anderen Produkte integriert. Zwar hat man auch auf diese Kritik eine Antwort mit einer neuen zukünftigen Architektur, aber das ist klare Zukunftsmusik. Bis dahin muss erst die Frage beantwortet werden, wie die Firma in den nächsten Wochen heißen wird. Der Vorstand hat klar seine Präferenz bekundet, den Enterprise-Bereich als letzten Überbleibsel des Com-Bereichs nach dem Deal mit Nokia ebenfalls auslagern zu wollen. Da mache man sich keine falschen Vorstellungen. Wer immer hier auch als übernehmender „Retter“ in Frage kommt, er hat bereits eine eigene Zukunftsarchitektur. Damit ist zu befürchten, dass jede Siemens-Lösung daraus bestehenden wird, die vorhandenen HiPath-Kunden zu übernehmen, mit dem Zugang zu CorNet eine saubere Migration in die eigenen Produkte zu schaffen und dann stufenweise den heutigen Siemensteil in 3 bis 5

## IP-Telefonie: die nächste Generation steht vor der Tür, Cisco und Siemens in der Sackgasse?

Jahren verschwinden zu lassen. Aus meiner Sicht unfassbar, dass ein Vorstand einen derartigen Zustand produzieren kann, der jeden Kunden ratlos im Regen stehen lässt. Ein klarer Affront des Siemens-Vorstands gegen seine bestehenden Kunden! Hier kann nur auch im Interesse der wirklich nicht zu beneidenden Siemens-Mitarbeiter umgehende Klarheit gefordert werden. Ist diese nicht schaffbar, dann bleibt den Kunden, die jetzt investieren wollen, wohl kein anderer Weg als der Wechsel zu einem anderen Anbieter. Aber das wird Dr. Kleinfeld wohl egal sein, er hat ja den Bereich inklusive der Kunden sowieso schon mental abgeschrieben. Deutschland darf sich hier wirklich bei seinen Topp-Managern bedanken, wieder einmal werden wichtige Zukunftstechnologien, die in Summe für den Standort Deutschland eine herausragende Bedeutung haben, einem völlig überzogenen Streben nach einer kurzfristigen Rendite-Optimierung geopfert.

Mit dem Funktionswechsel von der reinen Sprachkommunikation hin zu einer prozessorientierten Kommunikation erfolgt gleichzeitig der Wechsel von der Sprachwelt in die Kernwelt der IT. Simple Beispiel: ich muss dringend mit einem Kunden über ein wichtiges Dokument sprechen, ich rufe ihn per Button aus meiner laufenden Word-Applikation an. Mit der Annahme des Gesprächs ist das Dokument für ihn sichtbar. Das ist Dokumenten-Sharing, Synchronisation, Whiteboard-Funktionalität und was man sonst noch dahinter definieren möchte. Und damit ist man im Land der großen IT-Firmen, man ist im Hoheitsgebiet von IBM und Microsoft.

Nun werden IBM und Microsoft nicht bewegungslos zusehen, wie wichtige IT-Funktionen von Alcatel, Avaya, Cisco, Nortel, Siemens und anderen realisiert werden. Parallel haben sie eigene wichtige Probleme mit ihren Geschäftsmodellen zu lösen. Mal ehrlich, wer will Vista denn auf der Unternehmensebene wirklich haben? Wo ist denn der messbare monetäre Mehrwert? Vista ist aus meiner Sicht in vielen Bereichen auf den Konsumer-Markt optimiert worden, so wurde es auch von Gates und Ballmer auf den großen Kongressen der letzten Monate vorgeführt. Kaum eine der von ihnen präsentierten Funktionen macht für ein Unternehmen wirklich Sinn. Gleiches gilt für Office. Woher soll der Drang der Unternehmen zu Office 12 kommen, wenn die Mehrzahl aller weltweiten Unternehmenskunden Office 2003 noch nicht eingeführt hat? Das Zauberwort aus der Sicht von Microsoft

heißt nun Kollaboration. Zum einen werden die entsprechenden Funktionen als Basisarchitektur verankert, der Live Communication Server, der zugehörige Agent, Präsenzfunktionen, zentrale Datenbanken, die Erneuerung von Sharepoint-Services sind die Elemente dieser Architektur. Doch der eigentliche Köder für die Unternehmens-Kunden ist ohne Frage die Integration der ganzen Funktionalität in Word, Excel, Outlook usw. Damit wird Kollaboration zum Vehikel der Vermarktung von Vista und Office 12. Dazu gehört auch die Integration von Groove in die Office-Suite. Auf der Seite des Managements hat Microsoft diesen Wechsel und diese Neuausrichtung auch deutlich gemacht. Ray Ozie, der Erfinder von Notes, der Gründer von Groove, ist die personifizierte Neuausrichtung von Microsoft.

In der Kombination mit der Siemens HiPath 8000 wird nun ein Schuh daraus. Damit liefert Microsoft die Komplett-Lösung für Kommunikation aus einer Hand, von der Sprache bis zur Team-Kollaboration. Aus Sicht des Markt- und Analyseteams von ComConsult-Research bleiben dabei aber viele Fragezeichen bestehen. Bisher besteht die neue Microsoft-Welt aus unserer Sicht aus einer wilden Anreihung von zum Teil durchaus komplexen Tools. Wir erlauben uns, sowohl hinter den Investitions- als auch den Betriebsaufwand ein Fragezeichen zu setzen. Allerdings sind viele Details noch unklar. Microsoft hat angekündigt, die bisher wilde Funktionsansammlung sauber zu integrieren und

auch die magersüchtigen Sharepoint-Services zu einer brauchbaren Funktion zu entwickeln. Wir haben deshalb ein Analyse-Team aufgesetzt, das für unser großes Voice-Forum im November genau diese Frage analysieren wird.

Man darf auch nicht übersehen, dass Microsoft mit dieser neuen Strategie einen wesentlichen Mangel seiner Software-Architektur überspielen will. Nach wie vor basiert die Microsoft-Welt auf massiven Installationen auf dem Client. Die Möglichkeiten moderner Web-Architekturen werden nicht ausgenutzt. Damit entstehen sowohl signifikante Lizenz- als auch gerade Betriebskosten. Microsoft hat den Einstieg in Server- und Web-basierte Architekturen klar verschlafen.

Hier taucht nun IBM wie der Phoenix aus der Asche auf. Der Großrechner-Dinosaurier der 80er Jahre hat in den letzten 10 Jahren einen fast unglaublichen Wandel zum Marktführer moderner System- und Software-Architekturen vollzogen. Großunternehmen, die heute standortübergreifende Services einführen wollen, kommen an einer Evaluierung der IBM-Produkte kaum vorbei. Natürlich hat auch IBM den Zug der Zeit erkannt. Auch hier wird mit der Weiterentwicklung der vorhandenen Produktfamilien und deren Zusammenlegung an einer neuen Kollaborationswelt gearbeitet.

Wer wird dieses Spiel gewinnen? Mit dem Wechsel von der simplen Sprachkommu-

## Voice-over-IP-Forum 2006



**06.11. - 09.11.06  
in Königswinter**

Das ComConsult Voice-Forum ist die ComConsult-Spitzenveranstaltung des Jahres 2006.

Das Forum bietet in der optimalen und interaktiven Mischung aus

- Topvorträgen von ausgewählten Experten am ersten und zweiten Tag
- Podiumsdiskussion mit kritischen Fragen an die Hersteller
- Moderierte Produkt-Workshops am dritten Tag, Produkte und Konzepte im Live-Vergleich
- Vertiefungsthemen am vierten Tag
- Der begleitenden Ausstellung

Moderation: Dr. Jürgen Suppan

Preis: € 1.990,- zzgl. MwSt.\* (\*gültig bis 31.08.06)



Buchen Sie über unsere Web-Seite [www.comconsult-akademie.com](http://www.comconsult-akademie.com)

## IP-Telefonie: die nächste Generation steht vor der Tür, Cisco und Siemens in der Sackgasse?

nikation zur prozessorientierten Kollaboration haben die IT-Anbieter wie IBM und Microsoft auf den ersten Blick die besseren Karten. Sprachkommunikation kann theoretisch als kostenfreie Commodity-Lösung übernommen werden. Und Kollaboration funktioniert immer noch am besten, wenn es im Betriebssystem oder in der Server-Service-Architektur verankert ist. Schlechte Karten also für Avaya, Alcatel, Cisco, Nortel und Siemens? Auf den ersten Blick ja.

Auf den zweiten Blick ist die Lage komplexer. IBM und Microsoft leider unter Altsystemen, sie müssen dafür sorgen, dass jede Lösung rückwärtskompatibel ist. So wundert es nicht, dass die bisherige Microsoft-Architektur mehr an eine undurchsichtige Ansammlung von separaten Servern erinnert. Gleichzeitig sind IBM und Microsoft unter einem enormen Zeitdruck. Die mehrfache Verschiebung von Vista macht das deutlich. Zeit kann aber scheinbar dadurch gewonnen werden, dass man miteinander kooperiert und vorhandene Produkte anderer Hersteller integriert. Time-to-market ist damit deutlich geringer. Bestes Beispiel ist die enge Zusammenarbeit von Microsoft und Siemens. Aber sind die dabei entstehenden Monster wirklich das was wir wollen? Wer kann für dermaßen komplexe Produkte mit Unmengen undurchschaubarer interner Funktionsabhängigkeiten wirklich einen stabilen Betrieb garantieren? Was wir wollen sind sauber und klar strukturierte Betriebssysteme mit modernen Funktionen und Architekturen und keine Altsystemansammlungen mit kaschierenden Workarounds. Man betrachte den Unterschied zwischen Apple Mac OS X und Microsoft Windows um zu verstehen was ich meine (man darf dabei aber nicht vergessen, dass Apple an seinen Altsystemen wie OS9 fast zu Grunde gegangen wäre und nur das einmalige Glück, Next-Technologien inklusive Steve Jobs übernehmen zu können, hat die Firma gerettet. Aber die Botschaft ist klar: der konsequente Verzicht auf alle Altsysteme, der mutige Einstieg in eine völlig neue technische Basis hat OS X zu dem gemacht was es heute ist, dem ohne Frage mit Abstand besten Client-Betriebssystem auf dem Markt. Ob Microsoft-Kunden zu einem dermaßen massiven Schritt bereit und auch technisch in der Lage wären, darf ernsthaft bezweifelt werden).

Damit wäre die Ausgangslage für alle investitionswilligen Unternehmen ja schon komplex genug. Wie kann man sich hier richtig entscheiden, ohne dabei auf das falsche Pferd zu setzen? Immerhin geht es ja doch zum einen um sehr große Investition

tionen zum anderen aber auch um die konsequente Optimierung von wichtigen Betriebsabläufen. Und hier liegen immer noch gewaltige Einsparpotenziale.

Aber in der Tat haben wir einen wichtigen Funktionsbereich bisher nicht angesprochen. Dies sind die mobilen Endgeräte. Mobile Mitarbeiter benötigen mobile Endgeräte und haben immer mehr den Anspruch, an jedem Ort und zu jeder Zeit in alle wesentlichen Arbeitsprozesse ihres Unternehmens eingebunden werden zu können. Tatsächlich hat 3G/UMTS die mobile Arbeitsqualität um Dimensionen verbessert. Man darf auch nicht übersehen, dass diese Technologien auf den Märkten, die unsere Entwicklung treiben noch wesentlich wichtiger sind als bei uns. In den USA und Asien haben Geschäftsreisen eine völlig andere Dimension, sie sind häufiger, sie sind weiter und länger und sie finden zwischen verschiedenen Zeitzeitzonen statt. Von daher kommt aus diesen Kernmärkten eine erhebliche Nachfrage nach einer besseren Integration mobiler Mitarbeiter.

Technisch wachsen hier zur Zeit Wireless/3G und neue Dienste zusammen (Tripple Play als Konsumer-Beispiel). Auf der Endgeräteseite entstehen immer neue Formen von mobilen Geräten. Der Wald wird immer undurchsichtiger.

Wie können nun alle diese Trends und Entwicklungen in einer sinnvollen und wirtschaftlichen Strategie verheiratet werden?

den? Eine unglaubliche Herausforderung!

Wir stellen uns dieser Herausforderung mit dem ComConsult-Voice-Forum 2006 Anfang November in Königswinter. Unsere Analysten und Spezialisten arbeiten zur Zeit in diversen Projekten an dem Thema. Parallel haben wir eine Reihe wichtiger hausinterner Studien aufgesetzt, um gerade auch die Produkt- und Technologieentwicklung zwischen Alcatel, Avaya, Cisco, IBM, Microsoft, Nortel und Siemens bewerten zu können.

Das ComConsult-Voice-Forum wird mit diesen Analysen zu unserer wichtigsten Veranstaltung des Jahres 2006. Zögern Sie nicht, sich einen Platz auf dieser wichtigen Veranstaltung zu reservieren.

Parallel sind wir sehr an Ihrer Meinung interessiert. Schreiben Sie uns, wie Sie diese neuen Entwicklungen empfinden. Wie sehen sie speziell Cisco, IBM, Microsoft und Siemens und deren Auswirkung auf Ihr Unternehmen? Wir würden gerne eine Auswahl Ihrer Antworten im nächsten Insider veröffentlichen, Sie können natürlich wählen, ob dies namentlich oder anonym erfolgen soll.

Also: schreiben Sie an  
drsuppan@comconsult-research.com

Ihr  
Dr. Jürgen Suppan

## Voice-over-IP-Forum 2006



**06.11. - 09.11.06  
in Königswinter**

Das ComConsult Voice-Forum ist die ComConsult-Spitzenveranstaltung des Jahres 2006.

Das Forum bietet in der optimalen und interaktiven Mischung aus

- Topvorträgen von ausgewählten Experten am ersten und zweiten Tag
- Podiumsdiskussion mit kritischen Fragen an die Hersteller
- Moderierte Produkt-Workshops am dritten Tag, Produkte und Konzepte im Live-Vergleich
- Vertiefungsthemen am vierten Tag
- Der begleitenden Ausstellung

Moderation: Dr. Jürgen Suppan  
Preis: € 1.990,- zzgl. MwSt.\* (\*gültig bis 31.08.06)



Buchen Sie über unsere Web-Seite [www.comconsult-akademie.com](http://www.comconsult-akademie.com)

Neuer Kongress

# Voice-over-IP-Forum 2006

Die ComConsult Akademie veranstaltet vom 06. - 09. November erstmalig ihren neuen Kongress „Voice-over-IP-Forum 2006“ in Königswinter.

Das ComConsult Voice-Forum ist die ComConsult-Spitzenveranstaltung des Jahres 2006. Wir greifen die absoluten Top-Themen des Marktes auf und analysieren für Sie:

- Wo steht IP-Telefonie?
  - Funktionsumfang
  - Anlagen-Architekturen
  - Betriebsaufwand
  - Kostenentwicklung
- Wohin entwickelt sich der Markt in den nächsten 3 bis 5 Jahren?
  - Die ComConsult-Research-Marktanalyse
  - Neuer RFI und Positionierung von Produkten und Herstellern
- Welche Strategien verfolgen die großen Hersteller?
  - Welchen Einfluss werden speziell Microsoft und IBM auf den Markt haben? Was bedeutet die Integration von Voice und Kollaboration in Vista und Office 12 für den Markt?
  - Wie sicher sind die Produkt-



strategien von Cisco und Siemens?

- Eine neue Generation von IP-Telefonie kommt auf den Markt: wann kann gekauft werden, wann sollte die bisherige Technik zum Einsatz kommen?
- Voice-Konvergenz und ihr Nutzen im Unternehmen
  - Fixed-Mobile-Konvergenz
  - Roaming zwischen den Technologien
  - Entwicklung der mobilen Endgeräte-technik

- Vorteile und Risiken im Vergleich

- Anwendungs-Integration: vom Schlagwort zur Realität
  - Cisco Unified Communication in der Analyse
  - Was leistet der MS-Live-Communication-Server
  - Was machen die anderen Hersteller

- Voice-Security: Lösungsansätze im Vergleich

Das Forum bietet in der optimalen und interaktiven Mischung aus

- Topvorträgen von ausgewählten Experten am ersten und zweiten Tag
- Podiumsdiskussion mit kritischen Fragen an die Hersteller
- Moderierte Produkt-Workshops am dritten Tag, Produkte und Konzepte im Live-Vergleich
- Vertiefungsthemen am vierten Tag
- Der begleitenden Ausstellung

ein herausragendes Programm.

Zögern Sie nicht, sich einen Platz in dieser wichtigen Veranstaltung zu sichern.

Fax-Antwort an ComConsult 02408/955-399

Frühbucher-  
phase  
bis 31.08.06

## Anmeldung Voice-over-IP-Forum 2006

Frühbucher-  
phase  
bis 31.08.06

- ☐ Ich buche den Kongress  
**Voice-over-IP-Forum 2006**  
vom 06. - 09.11.06 in Königswinter  
zum Preis von € 1.990,-\* zzgl. MwSt.  
\*gültig bis 31.08.06  
(dann regulär € 2.190,- zzgl. MwSt.)

- ☐ Bitte reservieren Sie für mich  
ein Hotelzimmer  
vom \_\_\_\_\_ bis \_\_\_\_\_ 06

Vorname

Nachname

Firma

Telefon/Fax

Straße

PLZ, Ort

eMail

Unterschrift



Buchen Sie über unsere Web-Seite  
[www.comconsult-akademie.com](http://www.comconsult-akademie.com)

# Trouble-Shooting Forum 2006

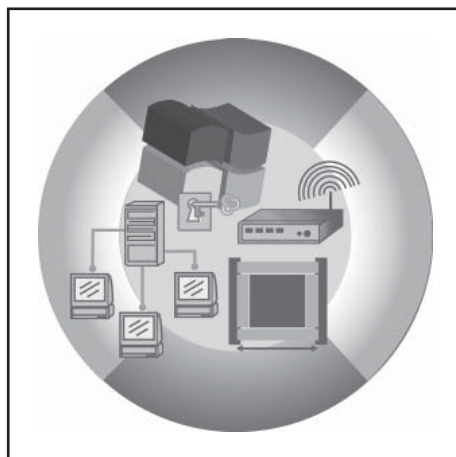
Die ComConsult Akademie veranstaltet vom 23. - 25. Oktober erstmalig ihren neuen Kongress „Trouble-Shooting Forum 2006“ in Neuss.

Leider laufen Netzwerke, Applikationen und Sicherheits-Infrastrukturen nicht immer so wie sie es im Idealfall sollen. Dabei gehören Totalausfälle noch zu den „angenehmen“ Störungen. Schlimmer sind Performance-Probleme und generell sporadisch auftretende und nur schwer reproduzierbare Störungen. Mit der immer weiter zunehmenden Abhängigkeit der Unternehmen von IT und Netzwerken ist deshalb das Thema Trouble-Shooting zu einem Top-Thema geworden.

Das ComConsult Trouble-Shooting-Forum 2006 ist unsere Top-Veranstaltung des Jahres zu diesem Thema. Seine Top-Themenbereiche sind:

#### Applikationen

- Bandbreite ist nur die halbe Miete: Die Laufzeit als begrenzender Faktor
- Neue Probleme im Umfeld von VPNs, Mobile und Co. (z.B. verringerte MTU, unkorrelierte Störungen von TCP bei Funk)
- Messung und Bewertung von Voice
- Wie wird man der großen Datenmengen Herr? Braucht man Spezial-Mess-technik im Anblick von Gigabit und 10 Gigabit?



#### Sicherheitsinfrastrukturen

- Problembereich Tunneling und Verschlüsselung: Messungen, Analyse, Überwachung und Fehlersuche
- Beispiel: Trouble Shooting von IPSec
- Beispiel: IEEE 802.1X
- Wenn Firewalls, Application Layer Gateways, Proxies und Intrusion Prevention Systeme nicht das filtern, was sie eigentlich sollten

#### „Management“ von Fehlern

- ITIL
- Prozesse zur Verhinderung von Fehlern (Configuration Management, Change Management), auch ein Fehler ist ein „Configuration Item“

- Wie kann schnell auf Fehler reagiert werden (Incident Management); effektive und effiziente Meldewege
- Sinnvoller Umfang externer Unterstützung beim Incident Management und beim (Business) Continuity Management.
- Dokumentation und Post Mortem Analyse

#### Last- und Stresstests

- Präventive Prüfung von Anwendungen und Netzelementen
- Vorgehensweise bei Last- und Stresstests
- Werkzeugüberblick

#### Funk

- Koexistenz verschiedener Funktechniken als Problem
- Aktuelle Messtechnik: Protokollanalyse, Spektrumanalyse, Überwachungstools
- Was leisten aktuelle Access Points für die Überwachung, was ist der Mehrwert spezieller Sensoren à la Airmagnet Sensor?
- Standortbestimmung mit WLAN? Wie arbeiten aktuelle Lösungen? Neue Ansätze.

Die Moderation der Veranstaltung erfolgt durch Dr.-Ing. Joachim Wetzlar, der seit über 10 Jahren zu den Top-Trouble-Shooting-Experten der Branche zählt.

Fax-Antwort an ComConsult 02408/955-399

Frühbucher-  
phase  
bis 30.07.06

## Anmeldung Trouble-Shooting Forum 2006

Frühbucher-  
phase  
bis 30.07.06

- ☐ Ich buche den Kongress **Trouble-Shooting Forum 2006** vom 23. - 25.10.06 in Neuss
- ☐ mit Workshop (am letzten Tag) zum Preis von € 1.790,-\* zzgl. MwSt.
- ☐ ohne Workshop (am letzten Tag) zum Preis von € 1.390,-\* zzgl. MwSt.  
\*gültig bis 30.07.06, dann erhöhen sich die Preise um jeweils € 200,-
- ☐ Bitte reservieren Sie für mich ein Hotelzimmer vom \_\_\_\_\_ bis \_\_\_\_\_ 06

Vorname

Nachname

Firma

Telefon/Fax

Straße

PLZ, Ort

eMail

Unterschrift



Buchen Sie über unsere Web-Seite  
[www.comconsult-akademie.com](http://www.comconsult-akademie.com)

## Notfallvorsorge für IT - flexibel und bedarfsgerecht

Fortsetzung von Seite 1



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 informatikorientierte Beratungsleistungen und Organisationsberatung im IT-Bereich. Zu diesen Themengebieten ist er regelmäßig als Referent bei der ComConsult Akademie tätig.

Wirft man einen Blick in eine vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe im Internet bereitgestellte Informationsbroschüre, so findet man am Ende der Einleitung die beiden maßgeblichen Kernfragen:

- Bin ich vorbereitet?
- Kann ich mir und anderen in Notsituationen helfen?

Genau diese Fragen muss sich auch derjenige stellen, der für die Verfügbarkeit von IT in einer Zielumgebung zuständig ist.

Die für das allgemeine „Notfallmanagement“ in Privathaushalten gedachte Broschüre gibt darüber hinaus noch einen guten Einblick in etliche grundlegende Aspekte, die dazugehören und auf die Situation in der IT übertragbar sind. So umfasst sie als Themen insbesondere „Vorsorge und Eigenhilfe“, „Prüfung des Vorrats“, „Notruf“, „Hochwasser“ und „Unwetter“.

Sich auf den Notfall aktiv vorbereiten, Notfallausstattung parat haben und gezielt zu wissen, wie man auf typische schädliche Ereignisse reagiert, all dies sind erste Punkte, die man auf die Notfallvorsorge im IT-Bereich übertragen kann.

Ebenso wichtig und übertragbar wird in der Broschüre die Zusammenstellung von im Notfall benötigten Dokumenten als Maßnahme benannt - und die Frage gestellt, ob diese Dokumente auch griffbereit sind!

Erinnert man sich an Notfallsituationen der jüngsten Vergangenheit, etwa Hochwasser-Situationen, so fällt auf, dass im Notfall auch eine besondere Rechtssituation herrscht. So ist nach offizieller Erklärung einer Notlage in vielen Ländern etwa

den zuständigen Stellen das Recht gegeben, zum Schutz von Leib und Leben Menschen zu zwingen, ihr Eigentum zurückzulassen und sich an einen anderen Ort zu begeben, als sie es aus freien Stücken tun würden.

Voraussetzung eines solchen Eingriffs ist aber die vorherige Schaffung einer entsprechenden Rechtsgrundlage. Überträgt man dies auf die Situation eines IT-Betreibers, so findet sich die Entsprechung z.B. in der Berechtigung, zur Schadensbegrenzung vorübergehend IT-Services außer Betrieb zu setzen, für deren Verfügbarkeit er normalerweise verantwortlich ist und in die Pflicht genommen wird.

Ein Beispiel in diesem Sinne kann eine Regelung sein, bei Sicherheitsvorfällen bestimmter Art vorübergehend den Internetzugang stillzulegen, bis geeignete Sofortmaßnahmen getroffen sind.

Wer hier erst im akuten Fall die Genehmigung zu einer solchen Sondermaßnahme einholen muss, verliert wertvolle Zeit, während der sich etwa eine neue, bislang unbekannte schadhafte Software ausgebreitet, vielleicht sogar über die eigenen Kommunikationskanäle auf Kunden oder Partner weiterverteilt hat. (siehe Abb. 1)

Eine Menge kann man also aus dem täglichen Leben bzw. dem Umgang mit allgemeinen Notfall- und Katastrophensituationen lernen, das auch auf die Notfallvorsorge in der IT sinnvoll Anwendung finden kann.

### 2. Notfälle in der IT: nicht völlig anders - aber mit Besonderheiten

Allerdings unterscheidet sich das Notfallthema im speziellen Fall der IT in einer Unternehmung andererseits zum Teil

deutlich von der Situation eines privaten Haushalts. Grundlegende Unterschiede, die dazu zwingen, erprobte Ansätze speziell auf die Gegebenheiten von Notfällen im IT-Bereich anzupassen, sind vor allem die folgenden:

- Übliche Schadensauslöser wie Feuer, Wasser, Stromausfall stellen nur einen Teil der möglichen Notfallursachen im IT-Bereich dar. Hinzu kommen
- IT-Sicherheitsvorfälle wie DoS-Attacken, Virenangriffe u. ä.
- Vorfälle, in denen der Datenschutz/ die Datenintegrität gefährdet sind
- Instabilitäten von IT-Installationen durch Software-Probleme
- schädliches Anwenderverhalten als auslösendes Ereignis sowie
- ein Wegfall der Vernetzung mit Dritten (WAN, Internet) als schädliches Ereignis.
- Ein Notfall im IT-Bereich ist nicht erst dann gegeben, wenn ein katastrophaler Zustand eintritt.

Im Grunde liegt bereits dann ein Notfall vor, wenn der durch den IT-Einsatz angestrebte Nutzen gravierend eingeschränkt ist. Dies ist schon dann gegeben, wenn festgelegte Wiederherstellungsfristen bis zum Normalzustand („Verfügbarkeitsanforderungen“) nicht eingehalten werden können. Solche Fristen sind gezielt so definiert, dass bei ihrer Verletzung unmittelbarer Schaden im Rahmen der durch die IT gestützten Vorgänge droht (z.B. Verletzung von maßgeblichen Liefer- o.ä. Fristen).

## Notfallvorsorge für IT - flexibel und bedarfsgerecht

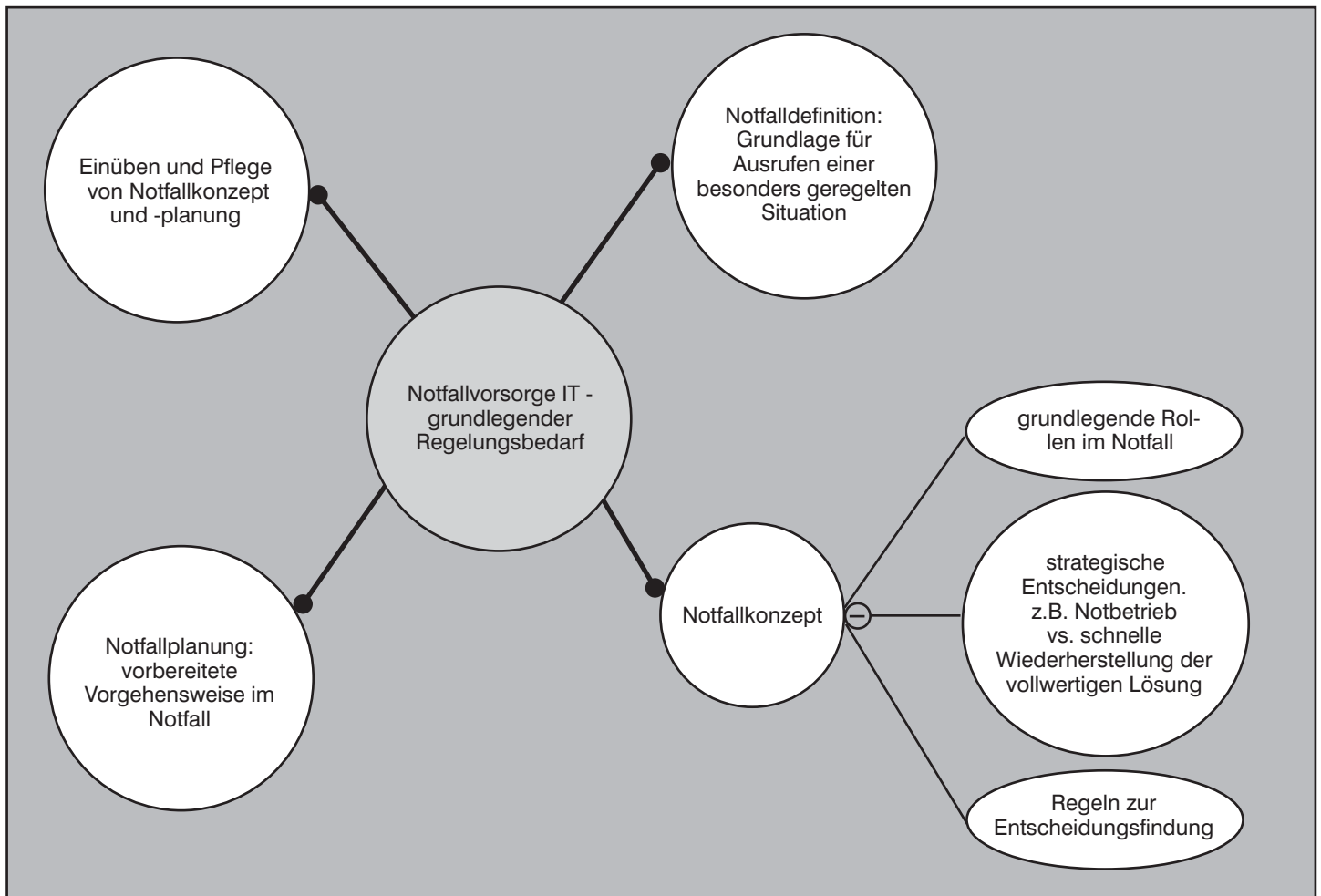


Abbildung 1: Notfallvorsorge - elementarer Regelungsbedarf (auch für IT)

- Häufig tritt eine Kettenreaktion ein, d.h. es gilt oft bei Vorfällen im IT-Bereich für die Bestimmung, ob ein Notfall eingetreten ist:
- Folgeschäden der unmittelbaren Beeinträchtigung sind für die Bewertung des Schadensausmaßes wichtiger als z.B. der reine Materialwert der betroffenen IT.
- Der für Unternehmensprozesse durch IT-Einsatz zu realisierende Mehrwert ist nur zu erzielen durch eine Kombination aus funktionierender Technik und kompetenter Nutzer.

Ein Beispiel in diesem Sinne ist die besondere Brisanz einer drohender Ausbreitung ansteckender Krankheiten:

IT-Arbeitsplätze im Bürobereich stehen hier durchgängig zur Verfügung, aber durch das Zusammentreffen der Anwender in ihrer gewohnten Arbeitsumgebung breitet sich die Krankheit wo-

möglich so stark aus, dass die kritische Anzahl arbeitsfähigen Personals unterschritten wird - dann nützt die IT auch nichts mehr.

In diesem Szenario kann man etwa gezielt zu der Möglichkeit greifen, einen größeren Teil des Personals über bereits vorhandene oder zügig zur Verfügung gestellte Heimarbeitsplatz-Anbindungen ihrer Arbeit nachgehen zu lassen, ohne der Ansteckungsgefahr im Büro bzw. auf dem Weg dorthin ausgesetzt zu sein. So kann das Risiko des akuten Vorfalls mit Mitteln der IT reduziert werden, und das, obwohl der Auslöser gar nicht im IT-Bereich liegt.

Dies funktioniert natürlich nur dann effektiv, wenn bereits fertige, erprobte Lösungen für VPN- oder RAS-Zugriff auf die zentralen IT-Lösungen des Unternehmens existieren. Wer jetzt erst solche Lösungen entwickeln muss (oder kurzfristig in großer Stückzahl notwendige Ausrüstung zu beschaffen hat, ehe die Lösung „in der Fläche“ greifen

kann), kann diese Maßnahme vergessen.

Insgesamt ist festzuhalten:

- Notfallsituationen in der IT sind nicht automatisch an einen „Großschaden“ als unmittelbaren Auslöser gekoppelt.
- Der Nutzungsausfall, d.h. Folgeschäden einer minderen oder Nicht-Verfügbarkeit von IT ist deutlich maßgeblicher für die Lagebewertung und das Schadensausmaß, als in anderen betroffenen Bereichen.
- Mögliche Notfallursachen und ihre Auswirkungen sind deutlich vielschichtiger, „normale“ Notfallauslöser und technische Pannen mit erhöhter Komplexität der Behebung addieren sich zu einer sehr unübersichtlichen Zahl von möglichen Notfallsituationen.

## Notfallvorsorge für IT - flexibel und bedarfsgerecht

Diese Besonderheiten führen dazu, dass es in der Unternehmenspraxis selten sinnvoll möglich ist, stereotyp mit gleichartigen Vorgehensweisen an die Aufgabe der Notfallvorsorge heranzugehen wie in anderen Bereichen wie Gebäudeschutz oder Notfallvorsorge im Gesundheitsbereich.

So ist es für die Notfallvorsorge in der IT nicht praktikabel, Notfallpläne in Form fertiger, umfassender Handlungsanweisungen für alle typischen Auslöser von Notfällen und alle sich hieraus möglicherweise ergebenden Schadensszenarien vorzubereiten.

Die gefährdeten „Güter“ und „Werte“ sind hochkomplex. Vernetzte, voneinander abhängige Technik, Datenbestände in ohne das Hilfsmittel IT nicht zugänglicher Form lassen sich nicht einfach durch Komfortverzicht im Notfall weiter nutzen, so wie man etwa notfalls zum Kochen vorgesehene Lebensmittel einfach kalt verzehrt.

Die Ausgangslage für ein geübtes Handeln von Notfällen ist somit im Falle der IT besonders kompliziert. Kommen noch im Notfall deutlich ungewöhnliche Zuständigkeiten oder lauter völlig „Normalbetriebs-unübliche“ Notfall-Lösungen und -Maßnahmen hinzu, so steht man sofort vor einer Kernfrage sinnvoller Notfallvorsorge:

**„Wer soll das „auswendig“ können bzw. mit erträglichem Aufwand über Hilfsmittel und gezieltes Training bewältigen?“**

Hier müssen geschickte Notfallkonzeption und Gestaltung der Falldokumente gezielt ansetzen.

### 3. Typische Schwächen von Falldokumenten in der Praxis

Der eingangs herausgestellte Regelungsbedarf muss praxistauglich geleistet und für die Umsetzung vorbereitet werden. Viele sind hier inhaltlich oder zeitlich überfordert und erledigen sich der Aufgabe der Notfallvorsorge für den IT-Bereich in Form einer saueren Pflicht, mit entsprechendem Ergebnis. In diversen ComConsult-Projekten waren immer wieder typische Schwachpunkte im Bereich der Notfallvorsorge zu beobachten:

- Unübersichtliches, „klobiges“ Falldokument

Beim Versuch, möglichst vielen wichtigen Schadensszenarien mit statischen Notfallplänen zu begegnen, entstand ein Werk, das unhandlich und abschreckend wirkt. Im Ernstfall hat ein solches

Hilfsmittel nur eingeschränkten Nutzen. Es wird nur zögerlich herangezogen und ist als schnelle Orientierungshilfe ungeeignet.

- nur der Katastrophenfall wird „ernst genommen“

Vielfach liegt Falldokumenten die erkennbare Haltung zugrunde, vorbeugende Maßnahmen seien ohnehin zwecklos. Es wird nur der K-Fall als Szenario gesehen, vor dem man sich mit Vorbeugung ohnehin nicht schützen könne. Der Aspekt der Notfallvermeidung wird wegen dieses Missverständnisses in der Notfallplanung grundlegend vernachlässigt, und das geschickte Ausnutzen entsprechender Lösungen auch im Falle, dass letztlich doch der Notfall eingetreten ist, geht nicht in die Notfallpläne ein.

- unnötige Abweichungen der Regelungen / Vorgehensweisen für Notfälle von solchen, die zum betrachteten Aspekt im Normalbetrieb gelten

Findet man dies vor, so hat meist ein „Spezialist“ für „K-Fallplanung“ oder „Business Continuity“ in Unkenntnis der genauen Lösungen für das Tagesgeschäft eine abweichende Vorgehensweise festgelegt. Dokumentationen der Lösungen für das Tagesgeschäft, etwa

Betriebshandbücher, waren ihm nicht zugänglich oder ihre Existenz nicht bekannt, und eine abschließende Prüfung durch die zuständigen Administratoren o.ä. hat, z.B. aus Zeitgründen, nie stattgefunden.

- nicht aktuelle Falldokumente

Leider ein Klassiker für jegliche Dokumentation. Die Pflege der Falldokumente wird so immer wieder zu einer Sonderaktion mit Projektcharakter, und zwischen diesen Projekten ist der Inhalt nicht verlässlich.

### 4. Tipps für die Gestaltung des Notfallmanagement in der IT

Wie verhindert man nun solche typischen Schwächen und kommt zu Notfallvorsorge mit resultierenden Dokumenten, mit denen es sich flexibel und angemessen auf die Vielzahl der möglichen Notfallszenarien im IT-Umfeld reagieren lässt?

Natürlich spielen immer die konkreten Gegebenheiten in der Zielumgebung eine Rolle, was Einzelheiten angeht. Ein paar grundsätzliche Tipps aus der ComConsult-Projektpraxis lassen sich aber nahezu überall sinnvoll verwenden und sollen im Weiteren zumindest angerissen werden, soweit dies im Rahmen eines kurzen Artikels sinnvoll möglich ist.

## Trouble-Shooting Forum 2006



**23.10. - 25.10.06  
in Neuss**

Leider laufen Netzwerke, Applikationen und Sicherheits-Infrastrukturen nicht immer so wie sie es im Idealfall sollen. Dabei gehören Totalausfälle noch zu den „angenehmen“ Störungen. Schlimmer sind Performance-Probleme und generell sporadisch auftretende und nur schwer reproduzierbare Störungen. Mit der immer weiter zunehmenden Abhängigkeit der Unternehmen von IT und Netzwerken ist deshalb das Thema Trouble-Shooting zu einem Top-Thema geworden.

Themenschwerpunkte:  
Applikationen, Sicherheitsinfrastrukturen, „Management“ von Fehlern, Last- und Stresstests, Funk

## Frühbucherphase bis 30.07.06

Moderation: Dr.-Ing. Joachim Wetzlar  
Preis: € 1.790,- zzgl. MwSt.\* (\*gültig bei Anmeldungen bis 30.07.06)



Buchen Sie über unsere Web-Seite [www.comconsult-akademie.com](http://www.comconsult-akademie.com)

## Notfallvorsorge für IT - flexibel und bedarfsgerecht

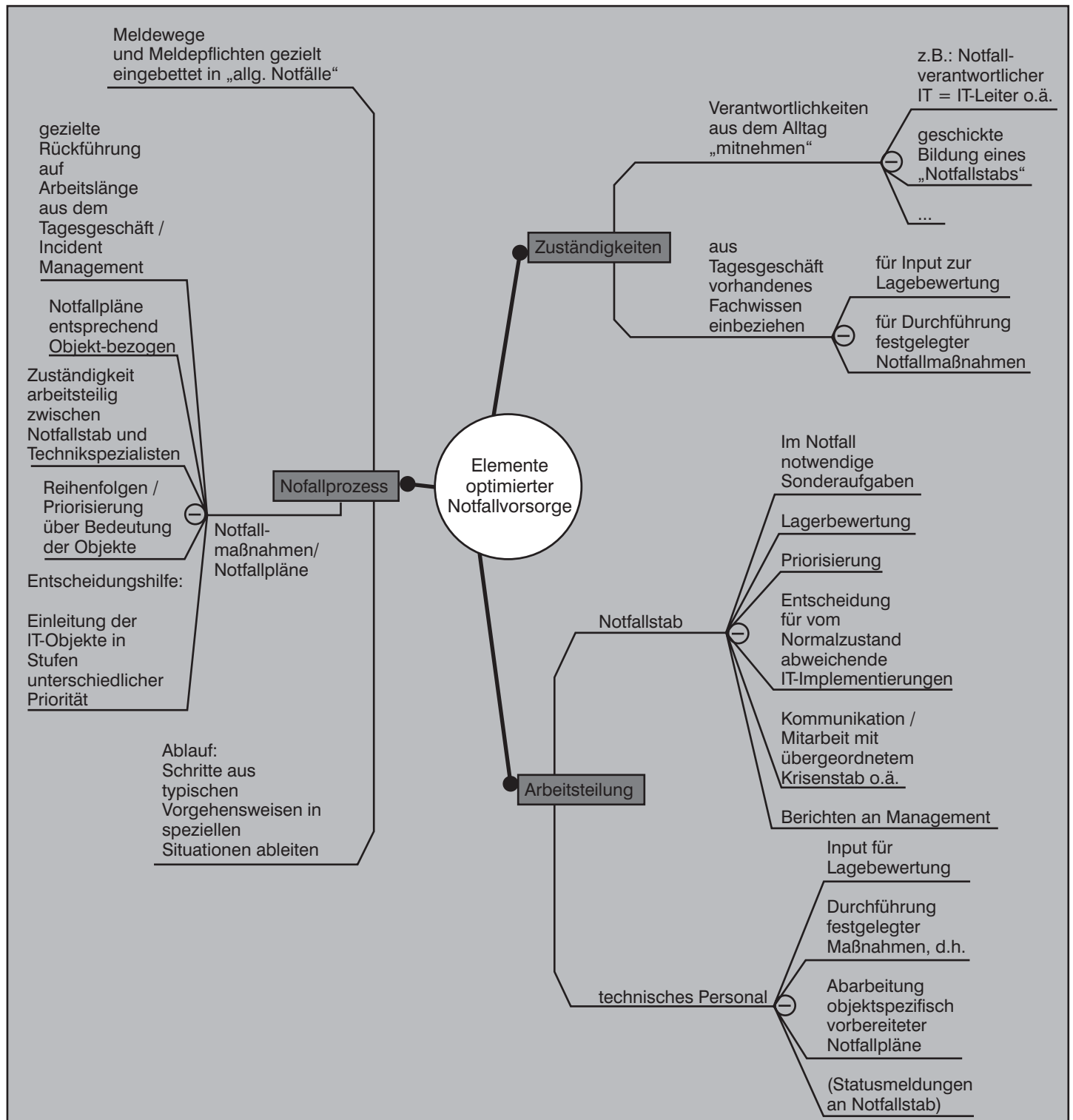


Abbildung 2: Notfallmanagement in der IT - Optimierungsansätze

Insbesondere ermöglichen sie eine gute Notfallvorsorge gerade auch in kleineren und mittleren Umgebungen, in denen es unwirtschaftlich wäre, ausgesprochene „Spezialisten“ für den Umgang mit Notfallsituationen herauszubilden, die dann bei Bedarf als eine Art IT-Katastrophenschutz eingreifen.

Auf einen kurzen Nenner gebracht, lassen sich die nachfolgend vorgeschlagenen Ansätze aus der ComConsult-Projektpraxis über folgende „Regeln“ charakterisieren:

1. Nicht unnötig vom normalen Alltag abweichen, auf diesen gezielt aufbauen.

2. Das Prinzip „teile und herrsche“ anwenden.

3. Auch im Notfall auf Arbeitsteilung zwischen Spezialisten für Koordination/ Entscheidungsfindung und Technik-Spezialisten setzen.

## Notfallvorsorge für IT - flexibel und bedarfsgerecht

4. Informationen nicht für Normalbetrieb und Notfalldokumente doppelt pflegen.
5. Die Aktualisierung von Notfalldokumenten übersichtlich gestalten.

Auch wenn viele der im Bild gegebenen Stichpunkte schon klar andeuten, was gemeint ist, sind noch einige Detailerläuterungen sinnvoll:

- Verantwortlichkeiten aus dem Alltag mitnehmen

Hier ist das Ziel, einen fließenden Übergang aus der Normalbetriebssituation in den formalen Notfallzustand und wieder zurück zu ermöglichen und dadurch Unsicherheit und Zusatzaufwand zu vermeiden.

Wird eine Person wie der RZ-Leiter, IT-Leiter o.ä. zum Notfallbeauftragten der IT ernannt, wird ein Kompetenzträger im Notfall eingebunden, der gemäß Eskalationsverfahren sicherlich ohnehin mit zu informieren wäre (kein zusätzlicher Meldeaufwand). Außerdem sind alle IT-Spezialisten gewöhnt, Weisungen und koordinierende Vorgaben von dieser Stelle zu akzeptieren und sich an diese Stelle zu wenden, wenn besondere Entscheidungen (Einsatz von Geld, außergewöhnliche Maßnahmen, ...) zu treffen sind.

Ebenso ist es geschickt, solche Personen auf die Kandidatenliste für den Notfallstab zu setzen, die in bestimmten zu Notfällen führenden Szenarien ohnehin maßgeblich beteiligt wären, so z.B. einen IT-Sicherheitsbeauftragten, wenn das Notfallszenario auf einen Sicherheitsvorfall zurückzuführen ist.

Ist nur die IT vom Vorfall betroffen und ein solcher typischer Auslöser gegeben, so reduziert sich der Notfallprozess auf eine definierte Vorgehensweise zum Umgang mit solchen Vorfällen. Bereits gelerntes Verhalten und an kleineren Notfallszenarien „geübte“ Schrittabfolgen können dann intuitiv auf größere Schadensszenarien übertragen werden, was den Aufwand für Notfallübungen und notwendige Kontrolle der Einhaltung des vorgeschriebenen Prozesses verringert.

- Arbeitsteiligkeit

Die Beschreibung der Kandidaten für Mitgliedschaft im Notfallstab lässt erahnen, dass diese im Tagesgeschäft nur bedingt über regelmäßiges Training zum Aufsetzen von Rechnern, Wieder-

herstellen von Datenbeständen u.ä. typischen Maßnahmen zur Beseitigung von Notfalldetails verfügen werden. Andererseits ist es bei Schäden größeren Ausmaßes kaum zu bewältigen, solche Maßnahmen in kürzester Zeit durchzuführen und zugleich für Koordinationsaufgaben, Meldung an Management und übergeordneten Krisenstab oder vergleichbare Aufgaben zuständig zu sein.

Insofern bietet sich eine Arbeitsteiligkeit an, bei der jeder das einbringt, für das er auch im normalen Tagesgeschäft vorrangig zuständig ist. Koordinierende und steuernde Aufgaben liegen bei den Mitgliedern des Notfallstabs, die Entsprechendes im Rahmen ihrer leitenden Funktionen auch im Alltag wahrnehmen. Dagegen liegt die effiziente Durchführung von Maßnahmen an der Technik in den trainierten Händen derjenigen, für die der Umgang mit dieser Technik zum täglichen Schwerpunkt gehört.

Weiterer Vorteil neben der geschickten Nutzung vorhandener „Skills“ liegt in der Tatsache, dass auch Notfallübungen zu einem gewissen Teil für die beiden Gruppen getrennt, sogar zeitversetzt ablaufen können.

- Voraussetzung: entsprechende Gestaltung der Notfallpläne

Folgt man den bisherigen Vorschlägen, so werden Notfallpläne folgerichtig mit Objektbezug gestaltet. Statt Notfallplänen je auslösendem Ereignis wird die Schadensfolge nach dem Prinzip „teile und herrsche“ auf die betroffenen IT-Objekte heruntergebrochen. Ziel eines Notfallplans ist es, durch typische Schritte und Maßnahmen einen bestimmten Teil der IT-Objekte gezielt wieder in einen Normalbetriebszustand zu versetzen.

- Priorisierung / Reihenfolgenfestlegung ebenfalls mit Objektbezug

Müssen vorübergehende Ressourcenprobleme gelöst werden, so bietet es sich bei Objekt-bezogenen Notfallplänen natürlich an, deren Abarbeitung in eine „geschickte“ Reihenfolge zu bringen. Hierfür gibt es zwei grundlegende Kriterien: Wichtigkeit des Objekts für die zu stützenden Arbeitsprozesse, und Abhängigkeit anderer IT von diesem Objekt (insbesondere: technisch notwendige Wiederanlaufreihenfolge).

Wie man hier einen systematischen Ansatz erhält, anstatt von Mal zu Mal Einzelentscheidungen für die jeweilige Liste „beschädigter“ Objekte treffen zu müssen, kennt man ebenfalls aus dem Normalbetrieb. So wird man etwa zur strategischen Festlegung von Überwachungsaufwand und -Häufigkeit im Rahmen automatisierter Überwachung (SNMP o.ä. Basis) Gefährdungsklas-

## Seminar



### Sicherheit 3: Praxis-Intensiv-Seminar zur erfolgreichen Konfiguration von Firewall, VPN, Windows-Clients, WLANs

Dieses 5-tägige Seminar vermittelt intensiv den praktischen Umgang mit Firewall, VPN, Windows-Sicherheit und WLAN-Sicherheit. Im Rahmen von praktischen Live-Übungen werden typische Konfigurationen analysiert und vermittelt.

Referenten: Markus Allelein, Dipl.-Inform. Oliver Flüs, Dipl.-Inform. Michael van Laak, Dipl.-Inform. Andreas Meder, Frank Neunzig, Sven Ossendorf  
Preis: € 2.290,- zzgl. MwSt.



Buchen Sie über unsere Web-Seite [www.comconsult-akademie.com](http://www.comconsult-akademie.com)

## Notfallvorsorge für IT - flexibel und bedarfsgerecht

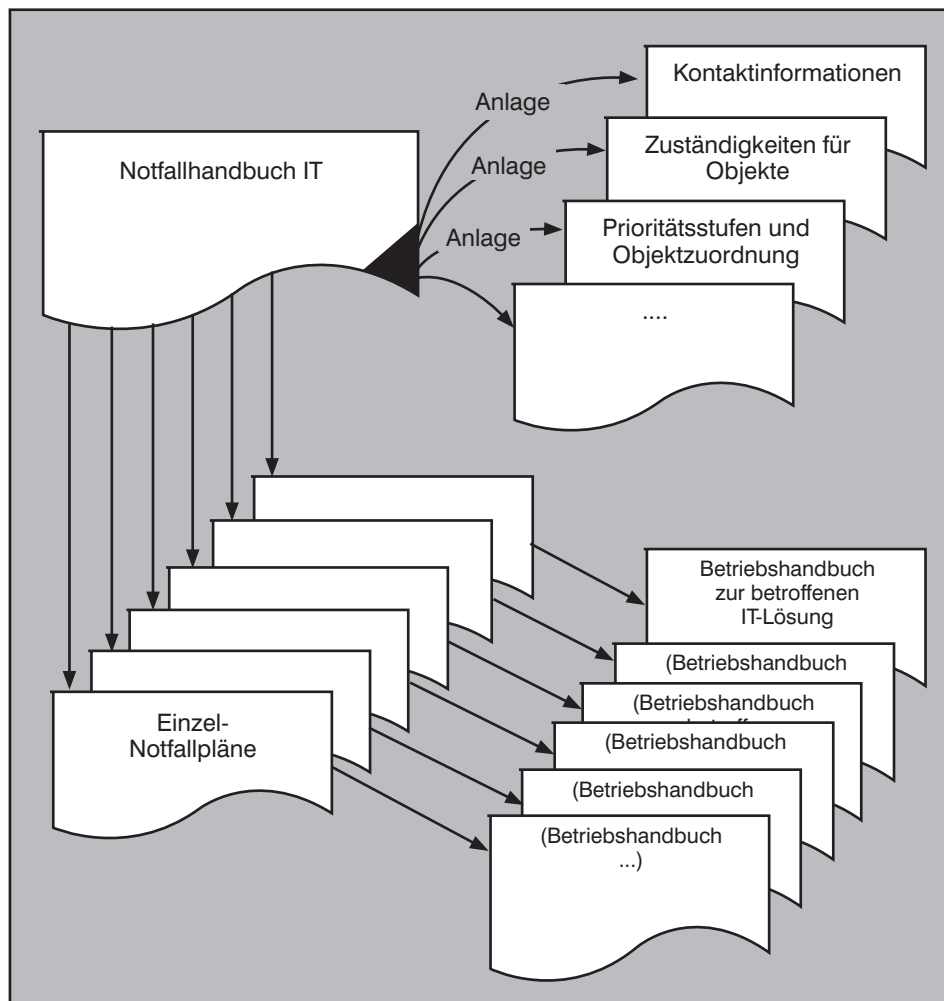


Abbildung 3: Modulare Handbuchgestaltung, aufbauend auf Betriebsdokumenten

sen bilden und die kritischen Objekte anders behandeln als die weniger kritischen. Nur konsequent, wer diesen „Klassifizierungsansatz“ auch für die Priorisierung im Notfall heranzieht ...

Bleibt die Umsetzung einer solchen Notfallkonzeption für die praktische Anwendung. Bindet man

- Notfalldefinition,
- besondere Festlegungen für Zuständigkeiten im Notfall,
- Beschreibung des Notfallprozesses mit Arbeitsteiligkeit und Zusammenarbeit über definierte Schnittstellen,
- notwendige Kontaktinformationen und
- Notfallpläne

in einem Dokument zusammen, so ist man schon auf einem guten Weg. Allerdings sollte man hierbei noch gezielt darauf hinarbeiten, sich das Leben bei der Pflege so einfach wie möglich zu machen und insbesondere keine Dinge im Notfallhandbuch noch einmal zu beschreiben

bzw. als Einzelinformationen aufzunehmen, die im Normalbetrieb ebenfalls gepflegt werden. Dies bedeutet:

- Für Vorgänge, die aus dem Normalbetrieb prinzipiell bekannt sind, wird auf entsprechende Dokumente zur Betriebsführung verwiesen (Betriebshandbücher, Laufzettel, etc.).

In einem Notfallplan wird auf solchen Betriebsdokumenten aufbauend nur dargelegt, soweit von der wohldefinierten Arbeitsweise des Normalbetriebs im Notfall abgewichen werden kann (z.B.: Verzicht auf Redundanz und zugehörige Konfigurationselemente; Verzicht auf Aktivierung bestimmter minder wichtiger Funktionalitäten auf ressourcenschwächerem Ausweichsystem - Notbetriebsform).

- Das gleiche gilt für Konfigurations- und Inventarinformationen.

Die Listung für den Normalzustand wieder bereitzustellender Hard- und Software nebst Soll-Konfigurationen gehört in Notfallpläne nicht als dort eigenständige Information, sondern wird per Verweis auf die IT-Dokumentation für den Normalbetrieb (CMDB) bedient. Diese Dokumentation erhält damit natürlich sofort hohe Priorität. Die Sicherung ihrer Verfügbarkeit auch im Notfall ist eine grundlegende Aufgabe der Notfallvorsorge, vergleichbar mit der zur Sicherstellung, dass das Notfallhandbuch selbstverständlich gerade im Notfall verfügbar ist!

Klingt bis hierhin alles völlig plausibel, wird aber in der Praxis längst nicht konsequent so gemacht ...

Gliedert man jetzt noch Informationen, die häufiger aktualisiert werden müssen als grundlegendere Festlegungen wie Prozessbeschreibung u.ä., bewusst in Anlagen aus, so lässt sich auch die Pflege des Handbuchs nach dem Prinzip „teile und herrsche“ vereinfachen. Kommt ein neuer Objekttyp hinzu (z.B. Server für eine neue strategische Applikation), so gibt es einen neuen Notfallplan sowie eine Ergänzung der Zuordnungsinformationen „Objekte zu Prioritätenstufen“. Werden Lösungen abgeschafft, erfolgt eine entsprechende Streichung von Handbuchelementen. Ändern sich nur Kontaktinformationen, wird eine entsprechende (auch gleich als Handzettel verwendbare) aktualisiert, der Rest vom Handbuch braucht nicht angeschaut zu werden; usw. (siehe Abbildung 3)

Man erhält eine modulare Handbuchstruktur, deren Pflege sich systematisch im Change Management verankern lässt, und ein Notfallhandbuch, das eine flexible Reaktion auf verschiedenste Notfallszenarien gut unterstützt:

Hat man erst mal das Schadenszenario auf schädliche Auswirkungen zu IT-Objekten analysiert und über im Handbuch festgelegte Regeln und Zuordnungen eine sinnvolle Reihenfolge zur Schadensbehandlung entschieden, so werden die entsprechenden Teile der entsprechenden Notfallpläne systematisch abgearbeitet und dabei notwendige Detailinformationen direkt aus den Betriebshandbüchern bezogen - ein zielgerichteter und bei aller Entscheidungskomplexität noch erträglich überschaubarer Weg zurück zum Normalzustand.

# VPN-Technologien: Alternativen und Bausteine einer erfolgreichen Lösung

Der komplett überarbeitete und neu aufgelegte Technologie-Report von ComConsult Research zeigt alle wichtigen Meilensteine bei Aufbau, Organisation und Betrieb einer VPN-Lösung. Die einzelnen Bausteine typischer Installationen werden anhand praxisnaher Vorgaben bewertet und ein umfangreiches Projekt- und Konfigurationsbeispiel detailliert besprochen. Insgesamt werden Sie somit in die Lage versetzt, Ihre eigene technisch und wirtschaftlich optimale VPN-Lösung zu entwerfen, in Ihr Gesamtkonzept einzubinden und zu betreiben. Lesen Sie im Folgenden einen Ausschnitt aus dieser Studie.

## 1.1 IPSec und das NAT-Problem

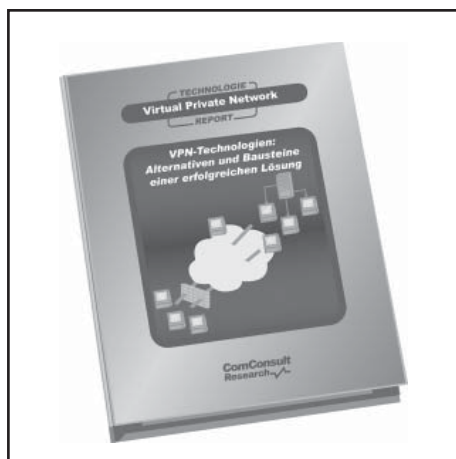
Der heute weit verbreitete Einsatz von NAT – hervorgerufen durch die Notwendigkeit, den knappen IPv4-Adressraum optimal zu nutzen, sowie aufgrund sicherheitstechnischer Vorteile bestimmter NAT-Varianten – hat beim Einsatz von VPN-Lösungen in der Vergangenheit meist für Probleme gesorgt, die erst seit Anfang 2005 durch standardisierte Mechanismen zumindest größtenteils behoben werden können. Dieses Kapitel behandelt Ursachen und Lösungsansätze dieses NAT-Problems.

### 1.1.1 Das NAT-Problem

Diverse Mechanismen von IPSec und NAT vertragen sich nicht miteinander. Insofern handelt es sich eigentlich nicht um ein NAT-Problem sondern um diverse NAT-Probleme. Wir wollen im Folgenden sukzessive diese Problembereiche untersuchen und beginnen bei dem offensichtlichen: dem Authentication Header.

#### Authentication Header

Der Authentication Header (AH) generiert eine kryptografische Prüfsumme über den Inhalt des IPSec-Pakets in Form eines Hashwerts, zu dessen Berechnung ein geheimer symmetrischer Schlüssel erforderlich ist. Dieser Hashwert umfasst alle im Paket befindlichen Daten mit Ausnahme des AH-Prüfsummenfelds und der nicht-statischen Informationen des IP-Headers. Da der Hashwert ohne Kenntnis des Schlüssels nicht gezielt gefälscht und der Schlüssel seinerseits aufgrund der Eigenschaften der Hash-Funktion nicht aus dem



Hashwert zurückberechnet werden kann, wird jegliche Manipulation am Datenpaket bei der Verifikation der Prüfsumme aufgedeckt und ein solches Paket vom Empfänger als ungültig verworfen. Der AH dient somit dem Erhalt der Integrität der übertragenen Datenpakete.

Unglücklicherweise basiert jedoch der NAT-Mechanismus bekanntermaßen genau auf einer gezielten Manipulation der IP-Adressen der Datenpakete: In der Regel wird die Absenderadresse durch eine andere Adresse ersetzt. Diese Manipulation wird vom AH äußerst wirksam unterbunden – er kann an dieser Stelle nicht zwischen erwünschten (NAT) und unerwünschten (IP-Spoofing) Manipulationen unterscheiden. Ein Einsatz des AH in NAT-Szenarien ist somit ausgeschlossen.

#### ESP und NAT/PAT

Dies allein scheint nicht weiter dramatisch, wird doch der AH in vielen Szenarien gar nicht verwendet bzw. kann meist darauf verzichtet werden, da das zweite IPSec-Protokoll, ESP, ebenfalls eine – wenn auch nicht ganz so weit reichende – Integritätsprüfung beinhaltet. Doch leider löst auch der Verzicht auf den Authentication Header das NAT-Problem nicht, denn auch ESP (Encapsulating Security Payload) verursacht Probleme im Zusammenspiel mit NAT. Ein generelles Problem sind hier multiplexte NAT-Kommunikationsbeziehungen.

Multiplexing ist bei NAT dann vonnöten, wenn mehrere interne Adressen auf eine (oder wenige) externe Adresse abgebildet werden müssen – das Standard-Szenario etwa bei der Verwendung von DSL-Routern im SOHO-Bereich. Üblicherweise kommt hier NAT (Network Address and Port Translation) zum Einsatz – dieser Mechanismus ist auch unter der Bezeichnung PAT (Port Address Translation) bekannt. NAT/PAT multiplexen durch gezielte Manipulation des Client-Ports (bei UDP bzw. TCP) oder anderer aus Sicht des Empfängers frei wählbarer Parameter (z.B. ICMP-Identifizierer). Durch eine eindeutige Zuordnung der jeweiligen internen Adresse zu einem solchen Parameter lassen sich die Antwortpakete gezielt demultiplexen.

Unglücklicherweise verschlüsselt ESP den Teil des IP-Pakets, in dem sich diese manipulierbaren Parameter befinden. Somit ist eine sinnvolle Manipulation nicht mehr möglich und das Verfahren scheitert. Einzige Chance – für entsprechend ausgestattete NAT-Geräte – wäre eine Nutzung des IPSec-Headers zum Multiplexen. Hier steht allerdings lediglich der SPI (Security Parameter Index) zur Verfügung, der wegen der in ESP integrierten Integritätsprüfung nicht manipulierbar ist. Freilich bestünde grundsätzlich die Möglichkeit, den originalen ISP zu verwenden – immerhin ist die Wahrscheinlichkeit einer Kollision aufgrund der 32 Bit Länge des SPI extrem unwahrscheinlich – allerdings besteht hier ein grundsätzliches Problem: der SPI wird für jede der beiden Kommunikationsrichtungen zwischen den beteiligten Partnern separat vereinbart. Die Folge davon ist, dass zwischen dem SPI der gesendeten Pakete und dem der empfangenen nicht notwendigerweise eine Korrelation besteht. Anders ausgedrückt: der Empfänger eines Antwortpakets kann aus dem darin enthaltenen SPI nicht mit Sicherheit die korrekte Adressabbildung ermitteln, da dieser SPI mit dem zuvor gesendeten in keinem erkennbaren Zusammenhang stehen muss.

Daher ist diese Methode nicht allgemein verwendbar; es gibt allerdings Produkte (beispielsweise von Cisco Systems), die in der Lage sind, identische SPIs auf beiden Seiten der Kommunikationsbeziehung si-

## VPN-Technologien: Alternativen und Bausteine einer erfolgreichen Lösung

cherzustellen, und somit ein NAT/PAT ermöglichen, solange die VPN-Lösung homogen bleibt.

**ESP im Transport-Modus**

Es bliebe somit - wenn überhaupt - nur statisches NAT, d.h. die feste Zuordnung externer zu internen Adressen - ein Ansatz, der in den meisten Fällen an zu knapp bemessenem offiziellem Adressraum scheitern dürfte. Zudem ist auch der Einsatz von statischem NAT nicht unproblematisch: Schwierigkeiten treten zumindest dann auf, wenn ESP im Transport-Modus verwendet wird (dies ist beispielsweise bei der in Windows2000/2003 integrierten IPSec-VPN-Lösung der Fall). Ursächlich hierfür ist der Prüfsummenmechanismus in TCP (teilweise auch in UDP), der neben den Source- und Destination-Ports auch die jeweiligen IP-Adressen von Sender und Empfänger berücksichtigt. Ändert ein NAT-Gerät eine IP-Adresse, so muss der TCP-Header, konkret: das Prüfsummenfeld, entsprechend angepasst werden. Ohne ESP stellt dies kein Problem dar, mit ESP jedoch sehr wohl, da das Prüfsummenfeld verschlüsselt ist. Eine Korrektur ist somit nicht möglich - sie würde von der Integritätsprüfung von ESP sofort entdeckt werden - was dazu führt, dass die Prüfsummenverifikation beim Empfänger scheitert und dieser derartige Pakete verwirft.

Dieses Problem tritt allerdings nur im Transport-Modus auf: Im Tunnel-Modus bezieht sich die TCP-Prüfsumme auf den inneren IP-Header, während die Manipulation am äußeren, dem Tunnel-IP-Header vorgenommen wird. Da dieser auch von der ESP-Integritätsprüfung nicht erfasst wird, kann in diesem Fall statisches NAT eingesetzt werden.

**IKE**

Somit bliebe also ESP im Tunnel-Modus mit statischem NAT als mögliche Verfahrensweise, die in diversen DSL-Routern im Übrigen unter der Bezeichnung „IPSec-Pass-Through“ implementiert ist. Unglücklicherweise hat jedoch auch IKE Probleme mit NAT; hierfür gibt es gleich mehrere mögliche Ursachen:

- IKE verwendet, abhängig von Einsatzform und Implementierung, IP-Adressen zur Identifizierung der Kommunikationspartner. Diese befinden sich als Parameter innerhalb des IKE-Protokolls. Stimmen diese Parameter mit den tatsächlichen IP-Adressen nicht überein, so wird ein entsprechendes Paket meistens verworfen.
- IKE verwendet selbst ebenfalls SAs, um einen geschützten Kommunikationspfad („IKE-Tunnel“) für das Aushandeln der IPSec-SAs bereitzustellen. Die zugehörigen IKE-SAs bestehen in aller Regel recht lange, um beispielsweise ein regelmäßiges Rekeying (dabei werden in bestimmten Zeitabständen die Schlüssel für die ESP-Verschlüsselung neu vereinbart) mit größtmöglicher Effizienz zu gestalten. Demgegenüber sind die NAT-Timeouts für UDP, dem von IKE genutzten Transportschicht-Protokoll, in der Regel erheblich kürzer. Da über IKE nur bei Bedarf Informationen ausgetauscht werden, kommt es häufig zu langen Idle-Perioden, die dazu führen, dass das Adress-Mapping aus der NAT-Table gelöscht wird, was zur Unzustellbarkeit der betroffenen IKE-Pakete führt.
- Nicht alle IKE-Implementierungen ak-

zeptieren Client-Ports, die vom Standard-Port (UDP 500) abweichen. Verändert ein NAT-Gerät den Source-Port eines abgehenden Pakets und der Empfänger akzeptiert nur den Port 500, so kommt keine Kommunikation zustande - die Aushandlung des IKE- und damit auch des IPSec-Tunnels scheitert.

Somit verbleibt oftmals nur die manuelle SA-Konfiguration, wenn NAT im Einsatz ist - ein Ansatz, der zumindest in umfangreicheren Szenarien absolut nicht praktikabel ist.

**Lösungsansatz: Encapsulation**

Das grundlegende Problem wurde natürlich schon vor geraumer Zeit erkannt und es existieren diverse Lösungen dafür, die jedoch allesamt proprietärer Natur sind. Allen derartigen Techniken ist gemeinsam, dass sie Encapsulation als Lösungsansatz verwenden, was nahe liegt, da sich damit - man sieht es beim ESP-Tunnel-Modus - einige Probleme quasi von selbst lösen.

Die meisten Hersteller generieren einen zusätzlichen UDP-Tunnel unter Verwendung verschiedenster Portnummern; eine etwas ausgefallene Lösung bot die (mittlerweile strategisch durch die XSR-Router ersetzte) Aurean-VPN-Lösung der Fa. Enterasys: Hier kam eine Verkapselung in HTTPS zum Einsatz, in der Hoffnung, auf dieser Basis aus vielen Netzwerken heraus ohne Anpassung einer etwaigen Firewall per VPN kommunizieren zu können. Dieser Ansatz wird im Übrigen auch von anderen Anbietern aufgegriffen, wenn auch nicht zur Behebung der NAT-Problematik: als Beispiel sei hier der so genannte Visitor Mode der Checkpoint VPN-1 genannt.

Fax-Antwort an ComConsult 02408/955-399

# Bestellung

## VPN-Technologien

☐ Ich bestelle den Report  
**VPN-Technologien: Alternativen und Bausteine einer erfolgreichen Lösung**  
 (Preis € 398.-- zzgl. MwSt. und Versand)

Vorname

Nachname

Firma

Telefon/Fax

Straße

PLZ, Ort

eMail

Unterschrift



Bestellen Sie über unsere Web-Seite  
[www.comconsult-research.de](http://www.comconsult-research.de)

# Service Level - Steuerung der Leistungs- qualität in der Praxis

Fortsetzung von Seite 1



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 informatikorientierte Beratungsleistungen und Organisationsberatung im IT-Bereich. Zu diesen Themengebieten ist er regelmäßig als Referent bei der ComConsult Akademie tätig.

Mit einer solchen Grundstabilität als Ausgangspunkt ist der Grundstein dafür gelegt, um eine wohldefinierte Service Güte einfordern zu können. Ob dies nun in einem als Service Level Agreement bezeichneten Dokument verankert wird, oder die entsprechende Vereinbarung anders niedergelegt ist, in jedem Fall ziehen sich Nutzer von IT-Lösungen immer häufiger darauf zurück, eine solche Lösung als fertiges, sofort verwendbares Paket von Leistungsinhalten „in Auftrag zu geben“ und zu verwenden. Die hiermit verbundene Rückbesinnung auf die eigentlichen inhaltlichen Aufgaben des Anwenders, für die er die entsprechende fachliche Ausbildung mitbringt, ist durchaus sinnvoll, weist doch die durchschnittliche IT-Umgebung mit Vernetzung, Sicherheitsaspekten und Software-Vielfalt mittlerweile eine Komplexität auf, angesichts derer ein mit

ganz anderen Schwerpunkten vorgebildeter Anwender beim Versuch der Selbsthilfe eher Schaden anrichten als vorwärts kommen wird.

Natürlich will sich auf der anderen Seite niemand blind darauf verlassen, dass seine notwendigen IT-basierten Arbeitsmittel auch wirklich so zur Verfügung stehen, dass sie ihm nützlich sind. Es ist eher wie mit Miet-Fahrzeugen: fordert man dort ein Fahrzeug einer gewissen Klasse mit Mobilitätsgarantie und möglichst reibungsloser Abwicklung der Formalitäten bei Buchung, Abholung und Rückgabe, so verlangt der IT-Anwender eine Lösung

- mit bestimmten Funktionalitäten,
- einer gewissen mechanischen und Software-technischen Stabilität,

- einem gewissen Komfort (Benutzerfreundlichkeit) sowie
- guter Unterstützung bei Bestellung, Problemen und Fragen der Nutzung.

Ungünstiger Weise lässt sich diese Summe von Forderungen nicht einfach über eine „Fahrzeugklasse“ und eine Mobilitätsgarantie fassen. Der Leistungsgegenstand ist technisch komplexer und vielfältiger in seinen Ausprägungen, und der Dienstleistungsanteil ist deutlich höher und vielschichtiger. Dies bedeutet entsprechend der im Bild gezeigten Aspekte für den Leistungsnehmer einen deutlich höheren Bedarf an genauer Festlegung, wie der Service aussehen soll. Der Dienstleister auf der anderen Seite sieht sich einer im Vergleich zum Mietwagenbeispiel deutlich komplizierteren Aufgabe der Organisation und Selbststeuerung gegenüber.

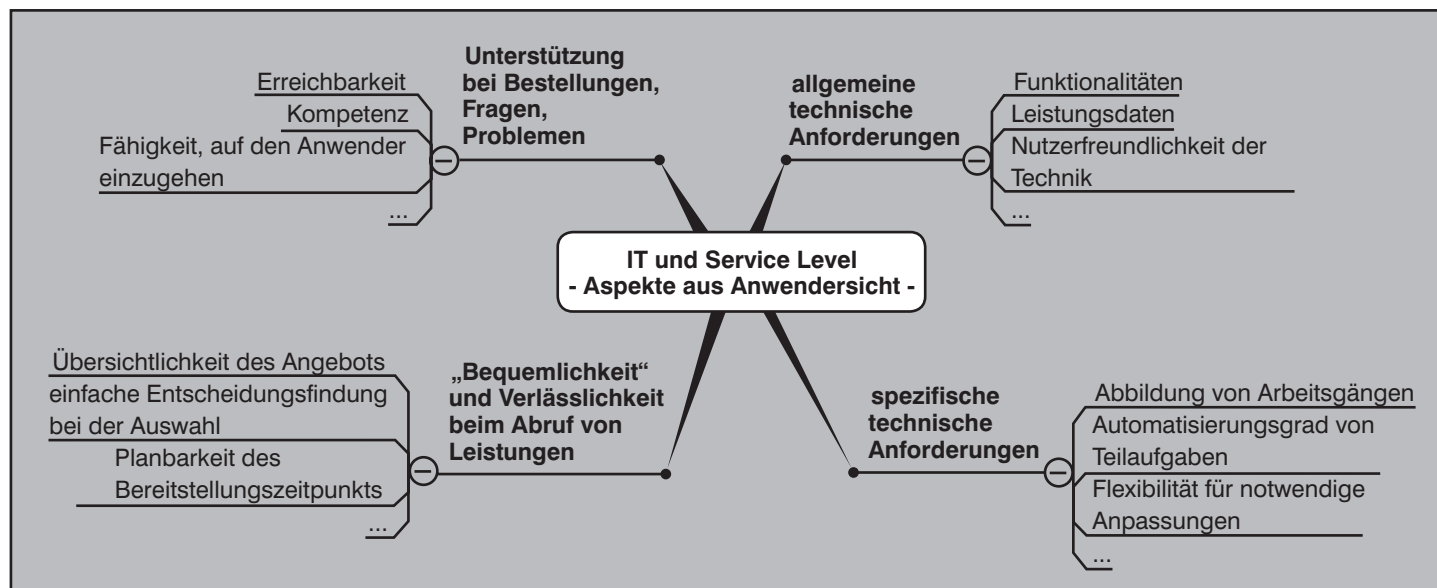


Abbildung 1: IT und Service Level - Aspekte aus Nutzersicht

## Service Level - Steuerung der Leistungsqualität in der Praxis

Was ist zu beachten, um mit dieser Situation erfolgreich fertig zu werden, welche in der Praxis als wichtig erkannte Aspekte und Ansätze zum Umgang mit diesen gibt es?

## 2. Service Level aus Sicht von Leistungsnehmer und Dienstleister

Vor dem dargelegten Hintergrund stellen Service Level-Definitionen aus Sicht der Praxis weniger ein Element der lästigen Verkomplizierung dar, sondern vielmehr die zwingend notwendige Leistungsdefinition, mit deren Hilfe

- der Leistungsnehmer seinen Bedarf so konkret wie nötig spezifizieren und die Einhaltung dieser Leistungsgüte auf Grundlage überprüfbarer Vereinbarungen einfordern kann
- der Dienstleister sinnvoll abgrenzen und organisieren kann, welchem konkreten Bedarf er zu entsprechen hat und verlässlich (Service Level) entsprechen kann.

Eine solche Service Level-Definition benötigt als Teil der „Spielregeln“ zwischen Leistungsnehmer und Dienstleister in der Praxis folgende typische Elemente:

- Messbare Vorgaben

Diese werden z.B. nach ITIL gerne als Key Performance Indicators (KPIs) bezeichnet. Ohne die hierdurch begründete Messbarkeit kann kein Service Level definiert werden - was nützt die Auflage, nicht zu schnell zu fahren, wenn man selbst entscheiden muss, was denn zu schnell sein könnte?!

- abnahmefähige Ergebnisdefinitionen

Hier sind alle technischen Anforderungen zu sehen, die nicht in bei der Nutzung unter Beweis zu stellenden Leistungsdaten bestehen, sowie geforderte Begleitdokumente bei Auslieferung etc.

Abnahmefähigkeit bedeutet die Möglichkeit einer systematischen Prüfung, ob die „Lieferung“ die geforderten Eigenschaften auch aufweist.

- eine wohldefinierte Schnittstelle zwischen Leistungsnehmer und Dienstleister

Es muss klar sein, wann, zu welchen Inhalten und in welcher Form der Leistungsnehmer auf den Dienstleister zugreifen kann und was als Reaktion auf solche typischen Zugriffe erfolgt.

So wird gesteuert, was der Dienstleister als Schnittstelle gewährleisten muss, aber auch, was der „Kunde“ an Disziplin aufweisen muss. Beispielsweise wird so der Klassiker „direkter Zugriff auf Durchwahl eines Technikers“ an Stelle der Nutzung geregelter Wege über einen Service Desk o.ä. Einrichtung ausgeschlossen (ansonsten droht sofort der Tod jeder garantierbaren Bearbeitungszeiten im Bereich des technischen Personals).

- Dokumentationspflichten

Teilweise muss der Leistungsnehmer bestimmte Dokumente über Anzahl und Zustand von IT-Objekten vorweisen können bzw. benötigt diese, um rechtzeitig Neubestellungen auszulösen o.ä. Teilweise muss über entsprechende Berichte eine Basis geschaffen werden, die Einhaltung des Service Level zu überprüfen.

- Regelungen für den Fall der Verletzung der Vereinbarungen

So ist nun mal der Mensch - keine Höchstleistung ohne „Herausforderung“. Die Praxis zeigt, dass noch so präzise Leistungsvereinbarungen das Papier nicht wert sind, auf dem sie stehen, wenn nicht auch klar ist, welche Folgen bei Verletzung dieser Vereinbarungen eintreten.

Dabei ist auch hierin nicht nur ein Mittel zur „Drangsalierung“ des Dienstleisters zu sehen. Vielmehr wird diesem die Möglichkeit gegeben, seinerseits ein kalkuliertes Risiko einzugehen. Ein Beispiel ist die Abwägung

- der einmaligen Zahlung einer Strafe im höchst seltenen Fall des Versagens eines noch erträglich bezahlbaren Lieferantenvertrags mit mittleren Lieferzeiten für Geräternachschub gegen

- eigenes Vorhalten teurer Geräte als Reservevorrat.

Natürlich muss der Leistungsnehmer allzu „großzügiger“ Risikoeinschätzung durch den Dienstleister entgegenwirken. Als brauchbares Stilmittel, das in der Praxis an der Reaktion der Externen spürbare Wirkung zeigt, ist die Forderung nach einem außerordentlichen Kündigungsrecht bei wiederholter Schlechtleistung.

## 3. Service Level(-Dokumente) und Auflagen von außen

Der Aspekt der Dokumentationspflichten ist mittlerweile so wichtig, dass es angezeigt erscheint, ihn nochmals aufzugreifen. In der Praxis ist hier ein Trend ersicht-

## Trouble-Shooting Forum 2006



**23.10. - 25.10.06  
in Neuss**

Leider laufen Netzwerke, Applikationen und Sicherheits-Infrastrukturen nicht immer so wie sie es im Idealfall sollen. Dabei gehören Totalausfälle noch zu den „angenehmen“ Störungen. Schlimmer sind Performance-Probleme und generell sporadisch auftretende und nur schwer reproduzierbare Störungen. Mit der immer weiter zunehmenden Abhängigkeit der Unternehmen von IT und Netzwerken ist deshalb das Thema Trouble-Shooting zu einem Top-Thema geworden.

Themenschwerpunkte:  
Applikationen, Sicherheitsinfrastrukturen, „Management“ von Fehlern, Last- und Stresstests, Funk

## Frühbucherphase bis 30.07.06

Moderation: Dr.-Ing. Joachim Wetzlar  
Preis: € 1.790,- zzgl. MwSt.\* (\*gültig bei Anmeldungen bis 30.07.06)



Buchen Sie über unsere Web-Seite [www.comconsult-akademie.com](http://www.comconsult-akademie.com)

## Service Level - Steuerung der Leistungsqualität in der Praxis

lich, der dem „Rückzug“ des Anwenders aus dem Feld der IT-Spezialisten gegenläufig ist: die Anwendung von Anforderungen von außen an die Sorgfalt und Verlässlichkeit des IT-Nutzenden im Rahmen seines Kerngeschäfts auf die IT-Ausstattung und mit ihr verbundene Dienstleistungen.

In einigen Fällen ist der Zusammenhang sofort nachvollziehbar, vor allem im Bereich von Sicherheitsanforderungen:

- Natürlich wirken sich Anforderungen im Bereich Datenschutz unmittelbar auf den IT-Einsatz aus, und die Notwendigkeit, geeignete Lösungen und Regelungen im Zweifel nachweisen zu können, betrifft natürlich auch eine IT-Dienstleistung.
- Wer sich unter Sicherheits-Gesichtspunkten besonders auszeichnen will oder muss, greift zum Hilfsmittel einer externen Auditierung, z.B. mit Zertifikat nach ISO 27001. Derartigen Prüfungen und Testierungen einer bestimmten Qualität aus Sicht der IT-Sicherheit können nur auf Basis dokumentierter Zustände und Arbeitsweisen erfolgen, da die tägliche Praxis mit sinnvollem Aufwand nur sehr stichprobenartig begutachtet werden kann. Auch hier ist der Gegenstand der Prüfung mehr oder weniger präzise der Umgang mit Informationen, mindestens das IT-Sicherheitsmanagement als Prozess zur Aufrechterhaltung eines bewusst aufgebauten Sicherheitsniveaus.

In anderen Fällen, die meist etwas Branchentypisches an sich haben, ist der Zusammenhang zur IT nur mittelbar herstellbar. So ergeben sich aus Vorschriften der für den Schutz der öffentlichen Gesundheit in den USA zuständigen „Food and Drug Administration“ FDA grundlegende Anforderungen an alle Unternehmen, die in den USA im Bereich der Marktbereiche Lebensmittel oder Arzneimittel tätig sind. Diese Anforderungen sind zunächst allgemeiner Natur, schließen aber insbesondere den Umgang mit Hilfsmitteln jeglicher Art ein. Ähnliches ist im Bereich Kapitalmärkte zu finden, siehe Basel II, den mindestens für alle an der US-Börse notierten Unternehmen relevanten Sarbanes-Oxley-Act u.ä.

Gerade bei solchen, die IT als ein Thema „unter vielen“ mit einschließenden Regelungen ist oft der Einfluss auf den Regelungs-, Qualitätssicherungs- und auch Dokumentationsumfang besonders groß. Man kann sich diesen Vorgaben kaum entziehen, da sie gesetzliche Auflagen darstellen oder umsetzen, bzw. branchen-

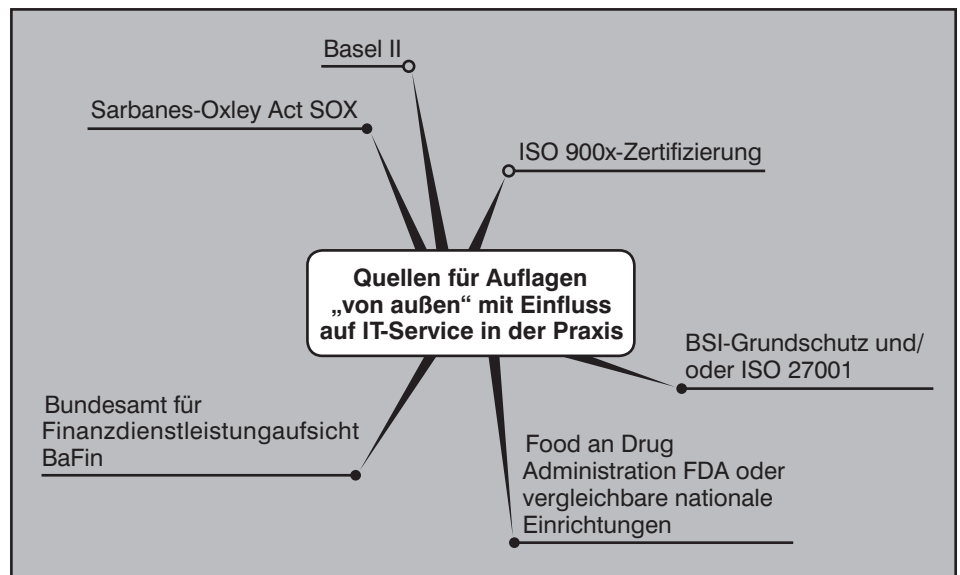


Abbildung 2: Risikomanagement-Anforderungen mit Einfluss auf IT-Service in der Praxis

typischen besonderen Bedarf an Risikomanagement abbilden. (siehe Abb. 2)

Der Aufhänger Risikomanagement erklärt auch die Maßgeblichkeit für IT und zugehörige Services. Um das Fahrzeugbeispiel noch ein letztes Mal zu bemühen: Wer seinen Fuhrpark für Gefahrguttransporte mit schlecht gewarteten Fahrzeugen bestückt, stellt ein besonders großes Risiko dar. Wer sich hier absichern will, wird als Teil der logistischen Leistung „Fuhrpark“ ausführliche Dokumentation sehen wollen zu Herkunft/ Vorgeschichte und Wartung/ Inspektion der Fahrzeuge.

#### 4. Steuerung von Service Güte - Art der betrachteten „Hilfsmittel“

Das vermehrte Aufkommen entsprechender Notwendigkeiten auch für den IT-Bereich, sichtbar in entsprechenden ComConsult-Projekten, war einer der wesentlichen Beweggründe für den vorliegenden Artikel. Der zweite Impuls war der verstärkte Rückgriff auf IT-Services auf outsourcing-Basis. Gilt es im Zusammenhang mit Auflagen von außen, diese Anforderungen möglichst geschickt, d.h. unter Vermeidung unnötigen Mehraufwands, mit der Steuerung der Service-Güte zu verbinden, so werden in der Praxis beim outsourcing leicht Fehler gemacht, die eine Qualitätssteuerung und -Sicherung erschweren oder sogar letztlich unmöglich machen.

Vor diesem Hintergrund und unter Berücksichtigung der bereits angesprochenen Gesichtspunkte werden im Weiteren Ansatzpunkte, Vorgehensweisen und Hilfsmittel betrachtet, die Definition und

Steuerung von Service-Qualität in der Praxis erleichtern und auf einen guten Weg bringen. Wenn dabei von Hilfsmitteln die Rede ist, sind hier nur nachrangig technische Lösungen gemeint, die gerne unter dem Oberbegriff Service Level Management-Werkzeuge o.ä. zusammengefasst werden. Diese werden als im ausreichenden Maße gegeben angesetzt und bedienen die Notwendigkeiten

#### • KPI-Messung

Aus Sicht des Leistungsnehmers wird hier die automatisierte und damit nur bedingt manipulierbare Gewinnung von Messdaten geleistet, auf deren Basis er die Einhaltung seiner messbaren Ansprüche überprüfen kann.

Aus Sicht des Dienstleisters wird hier die Möglichkeit geschaffen, sich rechtzeitig über negative Tendenzen mit Drohung der baldigen Verletzung von Service Level-Vereinbarungen klar zu werden, so dass er zeitig einschreiten bzw. seine Arbeitsweisen gezielt an den wirklich wichtigen Punkten verbessern kann.

#### • Berichtsgenerierung

Hier wird - je nach Berichtsinhalt für Leistungsnehmer, Dienstleister oder beide, eine „handliche“, übersichtliche und somit leichter auswertbare Aufbereitung von KPI-Messdaten geleistet. Ohne eine zumindest zu einem größeren Teil automatisierte Erstellung wären solche Berichte in der nötigen Häufigkeit nicht in wirtschaftlicher Art und Weise erstellbar.

## Service Level - Steuerung der Leistungsqualität in der Praxis

Derartige Hilfsmittel und durch sie erzeugbare Informationen werden also hier einmal als gegeben vorausgesetzt; Artikel im Insider wie auch Veranstaltungen der ComConsult-Akademie und Reports der ComConsult-Technologieinformation bieten hier weiterführende Informationen.

Mindestens genauso wichtig als „Hilfsmittel“ sind aber solche

- zur Präzisierung des Service Level bzw.
- zur Schaffung einer verlässlichen Basis für einen definierten Service Level.

Diese bedienen nicht die Notwendigkeit der technischen Überwachung des Zustands im Bereich IT-Dienstleistung, sondern greifen dort, wo dieser Zustand bewusst gesteuert werden soll bzw. muss,

um einen gewollten Service Level zu erreichen. (siehe Abbildung 3)

Hier wird die Frage beantwortet, ob „Service Level-Fähigkeit“ gegeben ist, oder anders formuliert: „Wie groß ist das (Rest-) Risiko, dass der gewollte Service Level nicht erzielt wird“? Mit dieser Formulierung ist auch erneut der Bezug zum Aspekt der Risikobetrachtung hergestellt. Es sollte daher gelingen, Fragestellungen der Steuerung von Service-Güte mit Auflagen gemäß äußerer Anforderungen zum Risikomanagement kombiniert zu bearbeiten.

### 5. Dokumente, Dokumente - wie soll man das alles pflegen?

Es muss auch zwingend so sein, dass man externe Auflagen und die eigenen

Notwendigkeit zur Steuerung der Service-Güte miteinander kombiniert bearbeiten kann. Ansonsten erstickt man bereits an der Fülle der zu erstellenden und zu pflegenden Dokumente, und hat keine Zeit mehr, die eigentliche Leistung zu erbringen:

Dokumentationsnotwendigkeiten zum Nachweis der Konformität zu Regelwerken wie z.B. ISO 27001, ISO 900x o.ä. stellen einen umfangreichen „Papierkrieg“ dar. Dieser ist tatsächlich in Papierform kaum noch sinnvoll handhabbar. Schon der Anspruch auf Aktualität verbietet fast schon die hauptsächliche/ vollständige Vorhaltung in Papierform, und die Nutzbarkeit als Arbeitsbasis in der Praxis auf Basis klobiger Ordnerwände ist fraglich. Angeht der so bildlich vorstellbaren Men-

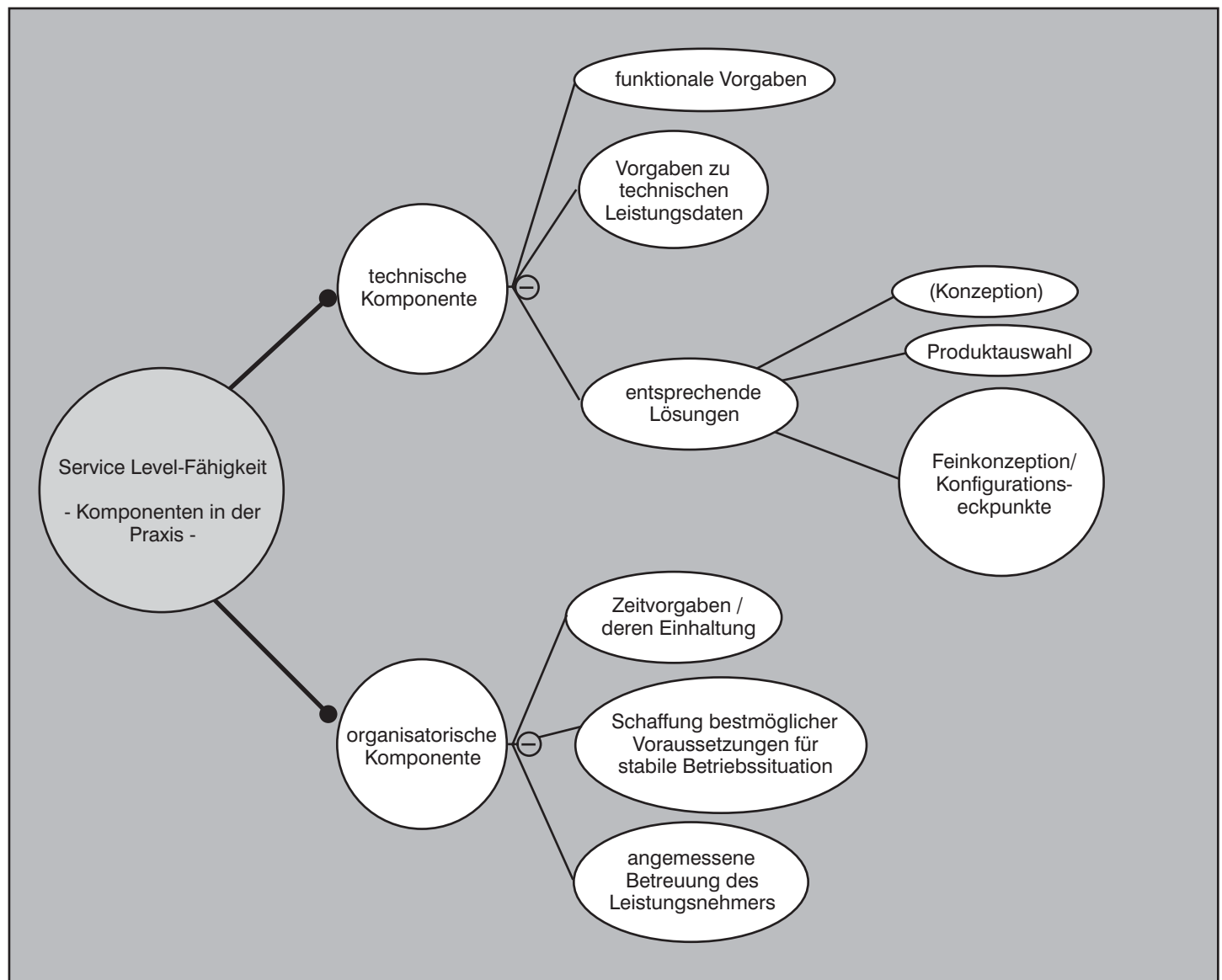


Abbildung 3: Praxis - Voraussetzungen für Service Level-Fähigkeit

## Service Level - Steuerung der Leistungsqualität in der Praxis

ge an notwendiger Dokumentation muss man sofort die Frage stellen, wie der Aufwand zur Pflege noch sinnvoll zu leisten. Die Antwort kann nur in einer Einbindung in ohnehin vorhandenen Aufgaben bestehen. Es hat wenig Aussicht auf Wirtschaftlichkeit und Machbarkeit, Dokumente im Rahmen der Service Level-Steuerung zu erzeugen, ebenfalls den erreichten Zustand zum Konformitätsnachweis einer Qualitätsanforderung hinsichtlich Risikomanagement o.ä. zu dokumentieren, und dies völlig unabhängig voneinander.

Vergleichbares gilt, wenn man IT-Leistungen „einkaufen“ will, die bestimmten Anforderungen an Service-Güte entsprechen sollen, die sinngemäß bereits aus anderen Gründen schriftlich fixiert vorliegen.

Wenn das Wort „Synergie“ auch arg abgegriffen ist - an dieser Stelle ist es für die

IT-Praxis eine Notwendigkeit.

Wie macht man das nun aber konkret?

In der Projektpraxis von ComConsult hat sich ein Ansatz bewährt, der sich die Tatsache zunutze macht, dass man im IT-Bereich mittlerweile gewohnt ist, in hierarchischen Dokumenten zu denken und mit diesen zu arbeiten. Das entsprechende „Training“ kam spätestens mit dem Internet. Es ist völlig normal und wird sogar als übersichtlich und damit hilfreich angesehen, eine größere Menge von Gesamtinformationen auf verschiedene „Seiten“ zu verteilen, die dann per Verlinkung untereinander zu einer nachvollziehbaren Hierarchie verknüpft werden.

Auf dieselbe Weise kann man einmal niedergeschriebene verbindliche Vorgaben zur Arbeitsweise im Bereich von IT-Dienst-

leistungen als einzelnes Dokument hernehmen und gleichlautend in verschiedene übergeordnete Dokumente einbinden (per Link, per formaler Nennung als „mitgeltendes Dokument“, etc.).

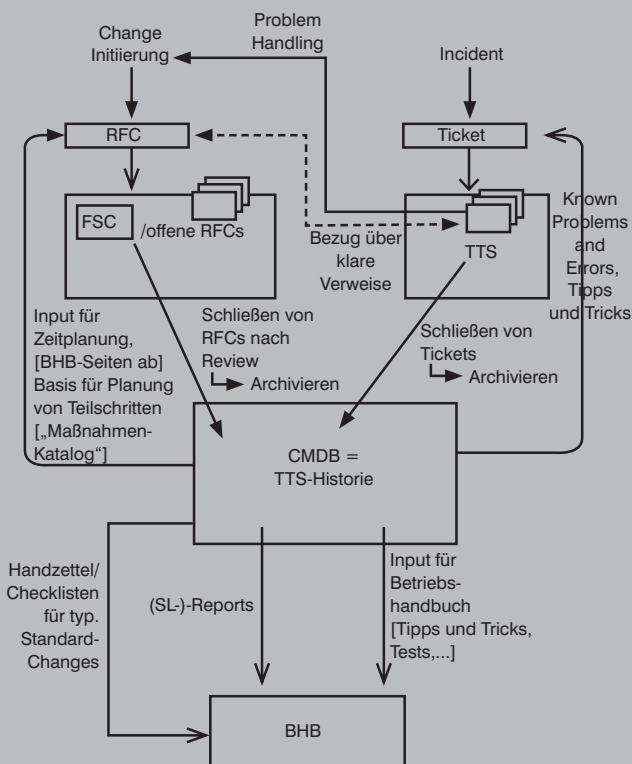
Man nehme etwa das Beispiel eines definierten Change Management-Konzepts. Eine Motivation hierfür kann man sich beinahe ersparen - der vielleicht größte Schaden in der Praxis kann im Rahmen einer „schlechten“, weil nicht oder ungeeignet geregelten Vorbereitung und Durchführung von Änderungen angerichtet werden. Entsprechend

- fordern praktisch alle Standards und Regelwerke zur planvollen Gestaltung von Services bzw. zum planvollen Risikomanagement die Definition eines allgemeinverbindlichen Change Management-Konzepts

## Konzept Change Management mit stabilem Service Level -

## Inhaltsverzeichnis

|                                                                                      |    |
|--------------------------------------------------------------------------------------|----|
| 1. Vorwort .....                                                                     | 4  |
| 2. Change Management-Konfiguration .....                                             | 5  |
| 2.1 Das Wesen des Change Management .....                                            | 5  |
| 2.2 Ansatz: Change Management in Anlehnung an ITIL .....                             | 6  |
| 2.2.1 Anlehnung an die Systematik, Adaption geeigneter Ansätze .....                 | 6  |
| 2.2.2 Übersicht: die ITIL-Management-Funktionen .....                                | 7  |
| 2.2.3 Einordnung Change Management, Ansatz des Konzepts .....                        | 8  |
| 2.2.3.1 Einordnung durch ITIL .....                                                  | 8  |
| 2.2.3.2 Konzeptansatz: Change-Management als Mittelpunkt (ITIL-unabhängig) .....     | 11 |
| 2.2.3.3 Abgrenzung Change-Management und Projekte .....                              | 12 |
| 2.2.4 Übersicht: wichtige Begriffe des Change-Management .....                       | 13 |
| 2.3 Wesentliche Komponenten eines strukturierten Change Management .....             | 17 |
| 2.3.1 Rollen und Aufgaben .....                                                      | 17 |
| 2.3.1.1 Change-Initiator, Annahme von Change-Initiativen .....                       | 17 |
| 2.3.1.2 Change-Advisory-Board CAB .....                                              | 20 |
| 2.3.1.3 Change Advisory Board / Emergency Committee (CAB/CE) .....                   | 23 |
| 2.3.1.4 Change-Manager .....                                                         | 24 |
| 2.3.2 Request for Change .....                                                       | 25 |
| 2.3.3 „Impact“-Analyse .....                                                         | 29 |
| 2.3.3.1 Gegenstand der Impact-Analyse .....                                          | 29 |
| 2.3.3.2 Hilfsmittel: Definition von Impact-Klassen .....                             | 32 |
| 2.3.4 Priorisierung, Wahl der Durchführungszeitpunkte .....                          | 36 |
| 2.3.4.1 Dringlichkeit als grundlegendes Kriterium .....                              | 36 |
| 2.3.4.2 Spezialfall „urgent“-Change .....                                            | 36 |
| 2.3.4.3 Zeitpunktwahl für „geplante Changes“ .....                                   | 39 |
| 2.3.4.4 Prioritäten von „non-urgent“-Changes .....                                   | 42 |
| 2.3.4.5 Details zum Umgang mit urgent-Changes .....                                  | 44 |
| 2.3.5 Zeitrahmen und grundlegende Schrittabfolge eines Changes .....                 | 45 |
| 2.3.5.1 (Erst-)Einstufung, Planung von Change-Vorbereitung und -Durchführung .....   | 45 |
| 2.3.5.2 Change-Autorisierung .....                                                   | 48 |
| 2.3.5.3 Change-Durchführung und Gesamtdauer des eigentlichen Change .....            | 48 |
| 2.3.6 Dokumentation / Veröffentlichung der Change-Planung, v.a. der Zeitpunkte ..... | 51 |
| 2.3.6.1 Forward Schedule of Changes „FSC“ .....                                      | 51 |
| 2.3.6.2 Projected Service Availability .....                                         | 52 |
| 2.3.6.3 Genehmigung von FSC- und PSA-Inhalten .....                                  | 52 |
| 3. Hinweise zur Change-Management-Praxis .....                                       | 54 |
| 3.1 Beziehung des Change-Managements zu anderen Management-Funktionen .....          | 54 |
| 3.1.1 Change-Management und Problem-Handling .....                                   | 54 |
| 3.1.2 Change-Management und Capacity-Management .....                                | 55 |
| 3.1.3 Change-Management und Configuration-Management .....                           | 56 |
| 3.1.4 Überblick: Zusammenhänge zwischen den Dokumentationen .....                    | 58 |
| 3.1.5 Change-Management und Release-Management .....                                 | 60 |
| 4. Literatur .....                                                                   | 67 |



BHB = Betriebshandbuch  
TTS = Trouble Ticket System  
SL-Report = Service Level-Reports

Abbildung 4: Change Management-Konzept - Beispielinhalte

## Service Level - Steuerung der Leistungsqualität in der Praxis

- fordert man in der Praxis bei kontinuierlich zu erbringenden externen IT-Dienstleistungen eine nahtlose Einbindung in das Change Management-Konzept des Auftraggebers und erklärt dieses zum Teil von Ausschreibungsunterlagen bzw. zum Vertragsbestandteil
- stellt die Einhaltung eines solchen definierten Change Management-Konzepts in der Praxis eine bindende Vorgabe für jegliche interne IT-Dienstleistung dar, wenn auf Risikominimierung bzw. mindestens durchschnittliche Service-Qualität Wert gelegt wird. (siehe Abb. 4)

Hat nun ein IT-Betreiber konkret

- im Rahmen von Nachweispflichten das Vorhandensein eines solchen wohldefinierten Change Management zu dokumentieren,
- dieses über entsprechende Verbindlichkeit zum Teil seiner Betriebsbasis zu machen sowie

- konkret Teilleistungen von Externen einzukaufen, die er in seine Gesamt-IT-Dienstleistung einbettet,

so kann er durch Einbindung eines einmal abgefassten Dokuments zur Spezifikation des Change Management in verschiedene Rahmendokumente die einmal gemachte Spezifikationsarbeit gleich mehrfach verwerten. Neben der Arbeitersparnis (Pflege nur eines Basisdokuments zum Change Management statt paralleler Versionen für verschiedene Zwecke) erreicht man so zudem noch eine Einheitlichkeit durch alle am Change Management beteiligten Instanzen. So wird es insbesondere in der Praxis für einen Auditor / Revisor aus Sicht eines Risikomanagement glaubwürdiger und plausibler, dass ein solches Change Management auch „gelebt“ wird und nicht nur als Papiertiger zu Zertifizierungs- oder ähnlichem Zweck geschrieben ist. (Was zur Abrundung noch fehlt, ist eine nachweisbare Vorgehensweise zur Einforderung/ Kontrolle der Einhaltung.)

Anmerkungen aus konkreter Projekterfahrung:

- Diese Verweisteknik kann insbesondere auch eingesetzt werden, wenn verschiedene Auflagen mit unterschiedlichen Schwerpunkten zu erfüllen sind. So gibt es im Bereich der SOX-Controls etwa einen Bereich zum Thema IT-Sicherheit. Hier kann gezielt auf eine parallel erfolgte Zertifizierung / Dokumentation gemäß ISO 27001 oder BSI-Grundschutz verwiesen und so der Nachweisaufwand auf einen solchen Querverweis nebst geringen Kurzerläuterungen reduziert werden. Erfolgt dies in nachvollziehbarer Weise, so wird es beim Audit akzeptiert.

- Oft sind Dokumente, die auf die dargestellte Weise auf gemeinsame Bestandteile zurückgeführt werden könnten, doch getrennt voneinander entstanden.

In diesem Fall zahlt sich eine Konsolidierung oft sofort in zweierlei Hinsicht aus. Zum einen wird natürlich das Ziel erreicht, zukünftig gemeinsame Textbausteine nur noch einmal pflegen zu müssen. Zum anderen wird bei der Bestimmung solcher „Doppler“ häufig auch überhaupt erst aufgedeckt, dass von vorneherein oder mittlerweile die verschiedenen Vorkommen der entsprechenden Thematik unterschiedlich, sogar widersprüchlich formuliert sind. Hier ist Klärungsbedarf aufgedeckt worden! Nach Festlegung, wie die Regelung zukünftig aussehen soll, kann diese Version dann als neuer, mehrfach eingebundener Baustein eine Aktion des Aufräumens und Beseitigens von Inkonsistenzen abschließen.

## 6. (Kontrollfragen zur) Bestimmung von Ansatzpunkten

Da im Zusammenhang mit Auditierungen das Stichwort „Kontrollfragen“ bereits gefallen ist - solche Kontrollfragen eignen sich in der Praxis auch gut als Hilfsmittel, den eigenen „Service-Zustand“ kritisch unter die Lupe zu nehmen.

Zunächst braucht man dafür zu kontrollierende Ziele. Für einen „funktionierenden“ Service Level sind dies etwa:

- klar und vollständig geregelte Zuständigkeiten (ohne drohen Situationen, in denen wegen Klärungsbedarfs Zeitvorgaben verletzt oder durch Parallelbearbeitung Ressourcen verschwendet werden)
- reibungsloses, zügiges Miteinander der verschiedenen Zuständigen und Beteiligten über wohldefinierte Prozesse (ohne drohen Durcheinander, unein-

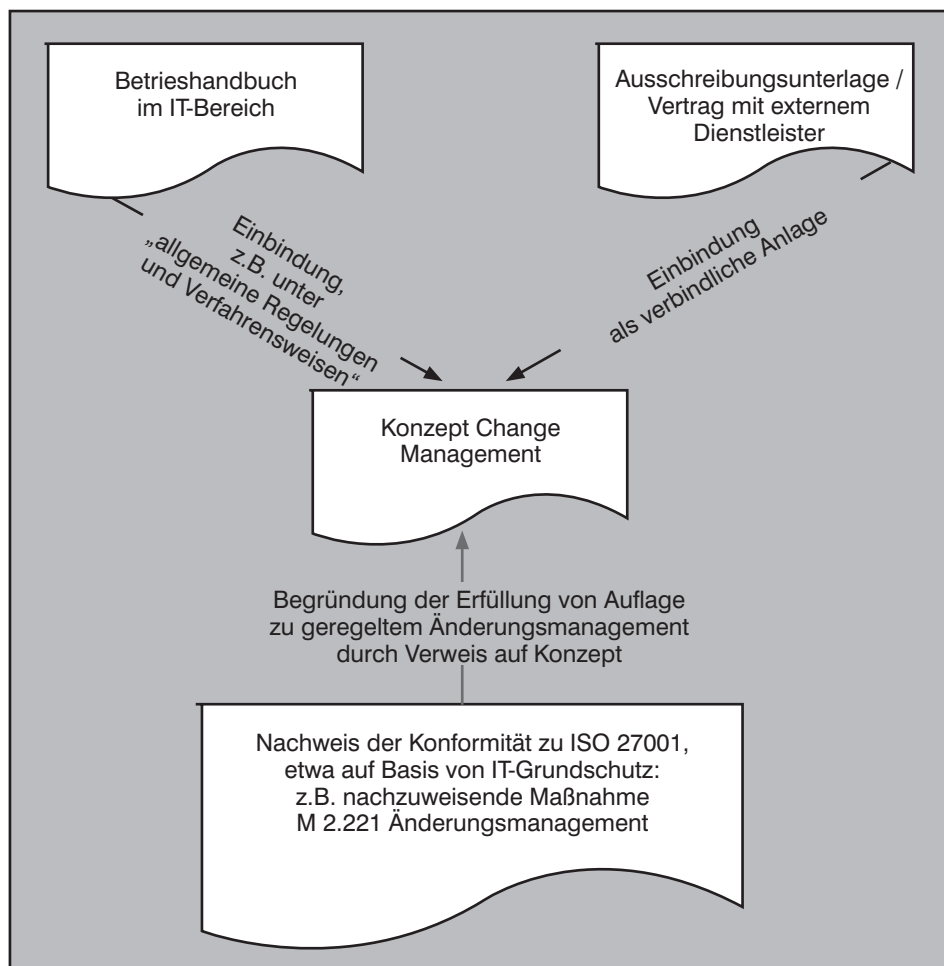


Abbildung 5: Einbindung eines Basisdokuments „Change Management“ an allen maßgeblichen Stellen

## Service Level - Steuerung der Leistungsqualität in der Praxis

heitliches Arbeiten mit zweifelhafter Ergebnisqualität, vermeidbarer Schaden durch zu spätes Einleiten notwendiger Maßnahmen, Unzufriedenheit des Leistungsnehmers wegen schlechter Betreuung usw.)

- einheitliche Arbeitsergebnisse (ohne erhöht sich unnötig und deutlich die Support-Komplexität, ist die Stabilität des IT-Gesamtverbunds fraglich – improvisierte Varianten statt getesteter Standardlösungen -, ist eine Abnahme deutlich erschwert und das Abnahme-Ergebnis kann von Fall zu Fall variieren).

Derartige Zieldefinitionen sind grundsätzlich anwendbar für Standard-Dienstleistungen im Tagesgeschäft, auf Support und Trouble Shooting mit Lösungszeitraum innerhalb gemäß Service Level noch erlaubtem Bereich liegen (Incident Management), und für außergewöhnliche Ereignisse wie Sicherheitsvorfälle oder Notfallsituationen, in denen die tatsächliche Problemdauer die gemäß Service Level-Vorgabe zulässige Länge überschreitet.

Die nachfolgenden Beispiele konzentrieren sich allerdings auf Tagesgeschäft und Support/ Trouble Shooting „im Limit“, da andernfalls der Service Level typisch ausgesetzt wird. Sicherheitsvorfälle, Notfälle oder gar Katastrophenfälle werden durch Ereignisse ausgelöst, für die einerseits ein unvermeidliches Restrisiko besteht, durch die andererseits eine Ausnahmesituation geschaffen wird, in der ein „normaler“ Service Level vorübergehend nicht sinnvoll aufrecht erhalten werden kann. Zum Teil muss sogar zur Schadensbegrenzung

gezielt der Servicegegenstand vorübergehend dem Leistungsnehmer vorenthalten werden: So wird etwa bei (vermuteter) Virenattacke der Zugang zum Internet vorübergehend deaktiviert, um die Attacke aufzuhalten bzw. einer rufschädigenden Weiterverbreitung an Dritte vorzubeugen.

Anmerkung aus der Praxis:

Nach Möglichkeit sollte die Befugnis zu derartigen Ausnahmen von der normalen Service-Verfügbarkeit vorab geregelt sein, bzw. zumindest ein Verfahren zur effizienten Abstimmung mit dem Leistungsnehmer und Freigabe durch diesen.

Nach Definition solcher zu erreichender Ziele wird dann durch zu diesen Zielen und der konkreten Umgebung passende Fragen die Service Level-Fähigkeit im Sinne der Zielerfüllung überprüfbar. (siehe Abbildung 6)

Je nach Umgebung und konkret eingesetzter IT / konkret definierten Service-Inhalten können nun gezielt Kontrollfragen definiert und überprüft werden. Diese ergeben sich aus dem Praxisalltag, indem nach Fällen gesucht wird, durch die einer der festgelegten Prüfaspekte gefährdet wird.

Beispiele (Wer mag, wende zur Klärung solcher Punkte die folgenden Beispielfragen einmal auf seine konkrete Situation an):

1. Schauen Sie sich zwei Endgeräte an, die von Personal im Bürobereich verwendet werden. Unterscheiden sich diese

- a) auf den ersten Blick völlig voneinander?
- b) nicht völlig, aber durchaus deutlich im Bereich bei beiden genutzter „Standard-Software“ (Konfiguration von Betriebssystem-Bestandteilen, Office, ...)?
- c) nur im Bereich von speziellen Anwendungen, die nicht grundsätzlich jedem Büroarbeitsplatz zur Verfügung gestellt werden?
- d) nur dann, wenn die Geräte nicht von der selben Person installiert worden sind?

2. Ein Access-Switch soll durch gleichartige Ersatzhardware ausgetauscht werden. Kann

- a) dies in einer garantierten Zeit durchgeführt werden, die bei vorhandener Hardware im Bereich von 1-2 Stunden liegt?
- b) überhaupt eine Vorhersage über die Ausführungsdauer gemacht werden?
- c) garantiert werden, dass das Austauschgerät nach Produktivsetzung in genau gleichem Konfigurationszustand ist wie das ausgetauschte?

3. Zur Erhöhung der Serverkapazitäten für einen bestimmten Server-Typ soll ein weiteres Gerät installiert werden, auf das zukünftig ein Teil der Anwender gezielt zurückgreifen soll. Kann die Installation dieses Servers

- a) nur vom für die bisherigen Server gleicher Art hauptverantwortlichen Administrator vorgenommen werden?
- b) auch von anderem Personal mit ver-

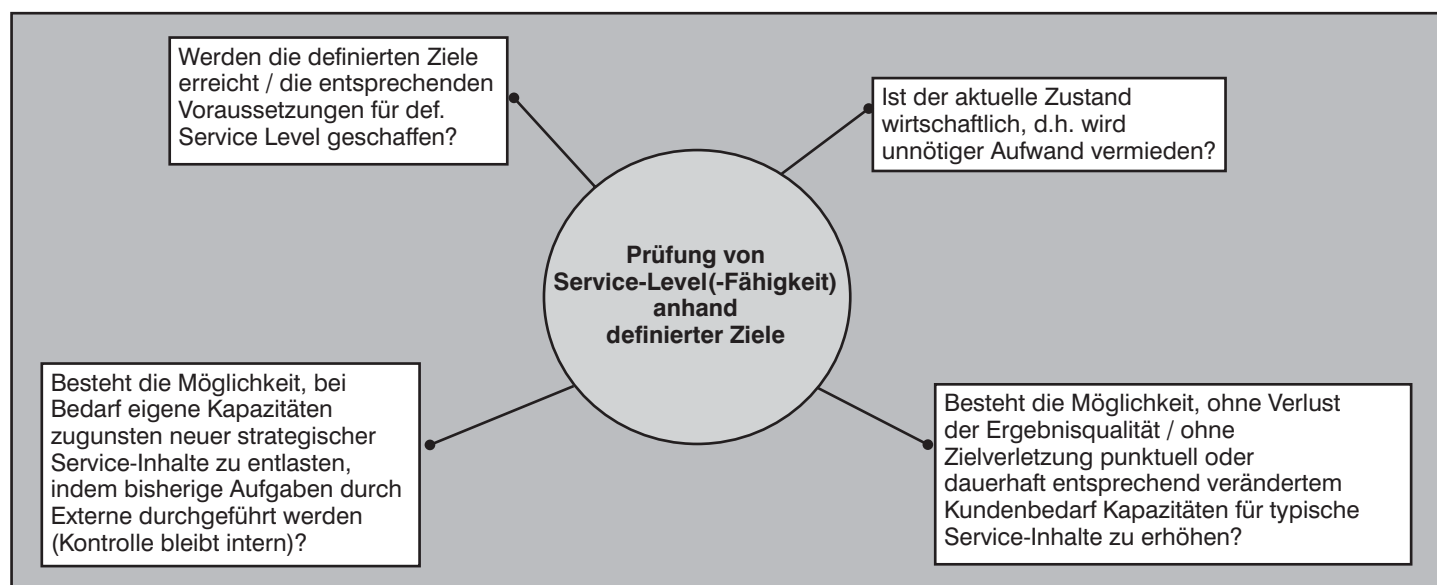


Abbildung 6: Grundlegende Prüfaspekte gemäß definierten Zielen

## Service Level - Steuerung der Leistungsqualität in der Praxis

- gleichbaren Grundkenntnissen übernommen werden, allerdings sieht der Server (Konfiguration) dann möglicherweise anders aus als die bisherigen?
- c) auch von anderem Personal mit ähnlichen Grundkenntnissen übernommen werden bei gleichem Ergebnis, ohne dass die benötigte Zeit indiskutabel ist?
4. Für eine Abteilung werden 10 neue Arbeitsplatz-Ausstattungen bestellt. Der Besteller
- a) wird über den konkreten Auslieferungstermin informiert, sofern die Geräte fertig sind. Solange der zugesagte späteste Termin nicht gefährdet ist, gibt es keine Informationen über Zwischenstände?
- b) kann auf Wunsch Informationen über erreichte Zwischenstände erhalten. Meldet er sich mit einer solchen konkreten Anfrage, werden für die Antwort notwendige Informationen schnell zusammengeholt und er erhält eine Prognose, wann die Auslieferung erfolgen wird?
- c) erhält auf Anfrage / in regelmäßigen Abständen sofort Informationen über den Zustand seiner Bestellung. Diese Informationen liegen an zentraler Stelle gesammelt und aktuell vor?
- d) kann selbständig über einen entsprechenden Zugang zu derartigen Informationen jederzeit kontrollieren, wie weit seine Bestellung bearbeitet ist?

Woher der Wind bei den verschiedenen Antwortmöglichkeiten aus Sicht erreichter Service-Qualität weht, ist wohl nicht erläuterungsbedürftig. Je nachdem, ob man auf Sicherstellung eines vereinbarten oder auf die Möglichkeit zum Anbieten eines neuen, höheren Service Level prüfen will, ändert sich selbstredend die Schärfe der Forderung, deren Erfüllungsgrad mit den Fragen geprüft wird. So erkennt man je nach Zielsetzung, ob man bestehende Vereinbarungen ausreichend gut erfüllt, bzw. wo die Grenzen der derzeitigen Arbeitsweise und Ausstattung liegen.

Zugleich deuten einige der gestuften Beispielantworten typische, in der Praxis immer wieder vorzufindende Schwachpunkte an, bei denen man gezielt ansetzen kann, um einen gewünschten Service Level zu ermöglichen bzw. auf wirtschaftlichere Weise zu realisieren.

Typische Problempunkte dieser Art sind insbesondere die folgenden:

- Es fehlen Standards für den Einsatz gleichartiger Software.

Teilweise auf Wunsch des einzelnen Anwenders, teilweise als eigene „Erfindung“ des jeweils eine Installation Durchführenden entstehen unterschiedliche Installationen gleichartiger Software.

Ist dies im Falle, dass hier kein Anwenderwunsch eingeflossen ist, eigentlich eine Dummheit, mit der man dem späteren Betreiber einer Installation das Leben unnötig schwermacht, ist ein allzu bereitwilliges Eingehen auf Anwenderwünsche zur „Optik“ o.ä. letztlich auch nicht im Sinne des Anwenderbedarfs.

Sofern sich solche Individualeinstellungen nicht automatisch (wieder-)herstellen lassen, hat der Anwender doch mit jeder neuen Installation (neues Endgerät, „Reparatur“ eines abgestürzten Rechners etc.) eine neue Oberfläche. Da kann er sich besser einmal an eine neue Standard-Gestaltung gewöhnen, die dann aber reproduzierbar ist.

In jedem Fall verlängert das Eingehen auf solche individuellen Wünsche zur Installation die durchschnittliche Dauer für den Installationsvorgang sowie den Aufwand für die Durchführung. Dies

wird sich letztlich negativ in der garantierbaren „Lieferzeit“ sowie im Preis für die Installationsleistung niederschlagen. Beides kann dem Anwender nicht recht sein.

- Es gibt keine festgelegte Standard-Vorgehensweise bei der Durchführung typischer Arbeiten.

Selbst auf Basis von „Musterkonfigurationen“ o.ä. als Endergebnis-Vorgabe wird der Weg, auf dem dieses Endergebnis herbeigeführt wird, unterschiedlich beschritten. Mindestens ist die Vorgehensweise abhängig vom jeweiligen Bearbeiter. Handelt es sich um Arbeiten, die der Einzelne nur unregelmäßig bzw. in längeren Abständen durchführt, kann sich sogar die Vorgehensweise sogar bei gleichem Bearbeiter von Fall zu Fall unterscheiden.

Das klingt erstmal unspektakulär, schließlich ist das Ergebnis doch per Vorgabe vordefiniert. Wer allerdings schon einmal selber mit Installationsarbeiten zu tun hatte, etwa unter Windows mit typischer Software wie Hardware-Treibern, Office, u.ä. hat da vermutlich andere Erfahrungen gemacht.

Im „günstigeren“ Fall überschreiben die nacheinander installierten Software-

## SEMINAR



## Internetworking: optimales Netzwerk-Design mit Switching und Routing 11.09. - 15.09.06 in Aachen

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

Referentin: Dipl.-Inform. Petra Borowka  
Preis: € 2.290,- zzgl. MwSt.



Buchen Sie über unsere Web-Seite [www.comconsult-akademie.com](http://www.comconsult-akademie.com)

## Service Level - Steuerung der Leistungsqualität in der Praxis

Pakete bestimmte Konfigurationseinträge, gemeinsam genutzte Software-Bausteine o.ä. nur in anderer Reihenfolge, und man hat auf den ersten Blick doch einen gleichartigen Rechner. Hier tickt jedoch eine kleine Zeitbombe, etwa für das Patch-Management. Aktualisiert man später eine solche Installation, kann es auf dem einen Rechner problemlos funktionieren, während es auf anderen, in anderer Reihenfolge installierten zu Verträglichkeitsproblemen kommt.

Im schlechteren Fall ändert man die Arbeitsreihenfolge in einer Weise, dass man plötzlich auf Fehler läuft und noch einmal von vorne beginnen kann - nachdem man jemanden nach seiner Vorgehensweise befragt hat, der die selbe Arbeit vorher ohne Probleme absolviert hatte.

Die Vorhersage einer garantierbaren Ausführungsdauer wird so natürlich schwierig.

- Existierende Informationen/ Unterlagen zur Durchführung von Arbeitsgängen sind „personengebunden“.

Das kennt vermutlich jeder, der schon mal in der Praxis „geschafft“ hat: die berühmten persönlichen Notizen. Selbst wenn sie lesbar in elektronischer Form vorliegen, muss man a) wissen wo sie zu finden sind und b) die gewählte Darstellungsweise auch richtig interpretieren. Aspekte wie Reihenfolge oder Hilfsinformationen sind oft nur für den Eingeweihten verständlich, d.h. den Erzeuger solcher Informationen.

- Unterlagen, die als Ergebnisdokumentation erzeugt werden, sind stark unterschiedlich je nach Bearbeiter.

Dies erschwert eine Abnahme ebenso, wie die weitere Verwendung solcher Unterlagen. Ehe man sie einer „Systemdokumentation“ als Basis für weiteren Betrieb und Trouble Shooting zuführen kann, müssen sie noch einmal überarbeitet, eventuell sogar ergänzt werden - eine Arbeit, die als „Nachbesserung“ aufwändiger ist als bei sofortiger Ausführung in brauchbarer Form durch den Installateur.

Derartige Schwächen in der Arbeitsweise und den als Hilfen gedachten „Arbeitsmitteln“ sind schon schädlich für kleinere Teilprozesse wie Installationsarbeiten an einzelnen Geräten. Hat man derartige „Individualitäten“ sogar im Bereich von Vorgängen, wo mehrere Bearbei-

ter kontrolliert und effizient zusammenarbeiten müssen, sind sie ein grundlegendes Risiko, und das nicht nur für die „Performance“ der Durchführung. Es können Sicherheitslücken entstehen, durch Missverständnisse doppelte Arbeit oder fehlerhafte Ergebnisse entstehen, die einer Abnahme nicht standhalten, bzw. es kann unnötiger Schaden entstehen, indem bei Stör- oder Sicherheitsvorfällen nicht rechtzeitig bzw. zunächst nicht korrekt reagiert wird.

Man sieht: zur Erreichung eines stabilen und wirtschaftlichen Service-Level (und nicht nur dafür) reicht eine Definition der Eckwerte eines einheitlichen Endergebnisses nicht aus, sondern wichtige Verhaltensweisen und Schritte müssen als „Prozesse“ einheitlich festgeschrieben und gelebt werden. Die entsprechende Festschreibung muss Klarheit schaffen hinsichtlich

- Verantwortlichkeiten / Zuständigkeiten
- Schrittabfolgen (Ablauforganisation)
- ggfs. einzuhaltender Detailvorgaben je einzeltem Teilschritt.

Wie dargelegt ist dies kein Akt der „Gängelung“ eigentlich für selbständige Arbeit kompetenter Fachleute, sondern eine Vereinheitlichung von Arbeitsabläufen und Verhaltensweisen

- zur Sicherstellung wirklich einheitlicher Arbeitsergebnisse als Basis effizienten Betriebs und effizienter Fehlersuche im Trouble Shooting
- zur Vermeidung unnötiger Probleme wegen Abweichung von einem getesteten Weg zum Ziel
- als Basis für Aufwands- und Kapazitätskalkulation
- als Basis für Zeitplanung und Ausführungszeitgarantien
- usw.

Wem in Ermangelung eigener negativer Praxiserfahrung zu definierten Zielen keine Kontrollfragen zur Bewertung der aktuellen Situation einfallen, der kann sich überlegen, was man im Ergebnis für Zustände erhält, die bei fehlender Klarheit im Sinne der geforderten Festschreibung für Ergebnisse eintreten können, und

- Betrieb und Trouble Shooting erschweren,
  - unerwünschte Probleme bei der Durchführung von „Routine-Arbeiten“,
  - Schwierigkeiten bei der Aufwandskalkulation bzw.
  - Probleme bei der Zeit- und Ausführungszeitschätzung o.ä.
- nach sich ziehen können - schon hat er

oder sie im Nu erste Beispiele für Auswüchse, denen es im Sinne der Service-Güte gegenzusteuern gilt, sofern sie in der überprüften Umgebung vorkommen.

Organisatorische „Hilfsmittel“, mit denen man gezielt so aufgedeckten Schwachstellen zu Leibe rücken kann (bzw. sie von vorneherein vermeidet), werden im Weiteren zumindest exemplarisch vorgeführt, inklusive der oben geforderten Möglichkeit einer „geschickten“ Kombination und Einbindung in ohnehin notwendige Dokumentationsaufgaben o.ä. Pflichten.

## 7. (Beispiele für) typische Steuerungsmittel

Während die bislang gebrachten Beispiele in Form von Kontrollfragen eher dazu gedacht waren, Schwachstellen aufzuzeigen, dienen die jetzt an ein paar Beispielen vorgeführten Mittel dazu, bewusst auf die Service-Güte einzuwirken. Ohne dass dies in jedem Fall noch ausdrücklich dargelegt wird, können derartige Mittel dabei sowohl für die eigene Selbststeuerung durch den Dienstleister verwendet werden, als auch zur Steuerung eingekaufter externer IT-Dienstleistungen. Dies muss auch so möglich sein: erst wenn man in die Spezifikation (möglicher) externer Dienstleistungen derartige Präzision hineinbringt, erhält man Vergleichbarkeit der Ergebnisse. Je nach Absicht des Herantretens an den Dienstleistungsmarkt wird auf diese Weise erst die Möglichkeit begründet, mit rechtfertigbarem Aufwand Vergleiche anzustellen:

- Externe Angebote werden so vergleichbar gemacht, dass man sich bei der Betrachtung von Preis-Leistungsverhältnis - nach einer gewissen Bereinigung im Falle von starker Übererfüllung im Einzelfall - tatsächlich auf den Preis Spiegel konzentrieren kann.

Verkürzt dargestellt:

- A. wer den Service Level nicht schafft, scheidet aus
- B. bei annähernd vergleichbarer inhaltlicher Angebotsgüte (d.h. keine große Übererfüllung des geforderten Service-Level) kann der Preis entscheiden
- C. gibt es bedeutende Preisunterschiede, die aber nachvollziehbar auf unterschiedliche angebotene Service-Güte zurückführbar sind, hat man grundsätzlich zwei Möglichkeiten:
  - a. den teureren, höhere Qualität An-

## Service Level - Steuerung der Leistungsqualität in der Praxis

bietenden darauf hinzuweisen, an welchen Stellen er inhaltlich „nachlassen“ kann, ohne auszuscheiden, und ihm Gelegenheit geben, auf dieser Grundlage ein modifiziertes Angebot inklusive neuem Preis abzugeben, oder

- b. intern zu entscheiden, ob einem die höhere Qualität erstrebenswert und bezahlbar erscheint und je nach dieser Grundsatzentscheidung die Angebotsreihenfolge abschließend festlegen.

Welchen dieser beiden Wege man geht, kann z.T. bereits vorgezeichnet sein, etwa wenn eine vorgeschriebene Vorgehensweise einen der beiden Wege verbietet (Vergaberecht mit Verbot von Nachverhandlungen im Fall a., bzw. strategische Auflage bestmöglicher Kostenreduktion im Falle b.).

Die Abfolge A. - C. mutet wie eine Kurzanleitung zur Beschaffung externer IT-Serviseleistungen an - und kann auch so genutzt werden, sofern eine wesentliche Voraussetzung erfüllt ist: eingehende Angebote basieren diszipliniert auf den Spezifikationen der Verdingungsunterlagen und fügen eigene Ausführungen nur da bei, wo diese dem Nachweis bzw. der Erläuterung dienen, dass bzw. wie man den so erhobenen Forderungen gerecht wird.

Leider besteht gerade bei Leistungen mit großem Dienstleistungsanteil eine immer wieder zu beobachtende Tendenz, dennoch mit eigenen formulierungstechnischen Gegenvorschlägen als Angebotstext zu antworten. Lässt man dies zu (bzw. muss dies im Einzelfall mangels Auswahl an brauchbaren Anbietern letztlich hinnehmen), so ist ein Vorgehen nach A., B., C. leider erledigt, und man muss in sehr diffizile Angebotsbewertung bzw. Detailverhandlungen einsteigen.

- Holt man externe Angebote zum Zweck eines Benchmarking, d.h. Vergleich mit der Alternative interner Leistungserbringung ein, so wird ein seriöses Benchmarking ermöglicht.

Erst durch die Auflage für den Externen, genau spezifizierte Leistungsinhalte und Leistungsqualität inklusive Einhaltung von Vorgaben zu Prozessdetails zu bepreisen, kann wirklich ein Marktpreis mit den Kosten interner Leistung verglichen werden. Mehr als ein von ComConsult zu bewertender Benchmarking-Versuch war in der

Projektpraxis nur bedingt aussagekräftig oder gar völlig unbrauchbar, weil es nicht gelang, den Vergleich von „Äpfeln mit Birnen“ zu verhindern. Fordert man nur Preise für „typische Leistungen“ in Schlagwortform ab, so bekommt man Preise für ein vom Anbieter typisch realisiertes Service-Niveau. Inwieweit dies mit dem intern geleisteten und tatsächlich benötigten übereinstimmt, so dass Preis-Leistungsverhältnis intern bzw. extern seriös vergleichbar sind, kann dann eigentlich nur „geraten“ werden. Dies ist weder eine sinnvolle Grundlage, eine strategische Entscheidung für outsourcing von (Teil-)Aufgaben vorzubereiten, noch dafür, Ansatzpunkte zu finden, wo man die interne Leistung auf Optimierungsmöglichkeiten aus wirtschaftlicher Sicht unter die Lupe nehmen sollte.

Was sind nun Beispiele für typische Hilfsmittel zur Steuerung der Service-Güte im Sinne dieser Sichtweise? Im Grunde ergeben sie sich unmittelbar aus weiter oben definierten Zielen / Ansatzpunkten sowie typischen Stilmitteln der Regelung organisatorischer Fragen - und erfüllen damit sofort auch Forderungen von externen Auflagen an Risiko- oder Servicemanagement, die gegebenenfalls zu erfüllen sind.

Je nach Bedarf und benötigtem Detaillie-

rungsgrad werden

- Zuständigkeiten festgeschrieben
- Arbeitsabläufe auf Prozessebene bzw. auf der Ebene einzelner Arbeitsgänge hinsichtlich Schrittabfolge und zu beachtenden Details festgeschrieben und
- Begleitdokumente vorgegeben/ Templates oder Standardformulierungen erarbeitet, die sowohl die Einhaltung der Festlegungen zum Arbeitsablauf erleichtern als auch als Dokumentation zu Nachweiszwecken bzw. als weitere Betriebsbasis dienen können.

Da der Sprachgebrauch für die Dokumente solchen Inhalts variiert, besteht hier die Gefahr, Verwirrung auszulösen. Wahlweise werden Begriffe wie Policy / Service Operating Procedures, Richtlinien/ Verfahrens-anweisungen, Dienstanweisungen / Arbeitsanleitungen o.ä. verwendet.

Im Rahmen des vorliegenden Artikels werden eher beschreibende Begriffe benutzt, die dann sinngemäß in die jeweilige Sprachregelung der Zielumgebung zu übersetzen sind:

- Rahmenrichtlinien

Diese regeln grundlegende Aspekte auf einer sehr allgemeinen Ebene, zum

## SEMINAR



## Sicherheitsmechanismen für Voice over IP

### 19.10. - 20.10.06 in Köln

In diesem Seminar wird vermittelt,

- was sich in Bezug auf Informationssicherheit mit der Umstellung auf VoIP ändert,
- welche Gefahrenpotenziale berücksichtigt werden müssen,
- welche Standards für VoIP-Sicherheit relevant sind,
- wie die Vertraulichkeit der Sprachkommunikation in IP-Netzen geschützt werden kann,
- worauf beim Design von VoIP-Umgebungen hinsichtlich Verfügbarkeit zu achten ist,
- wie die IP-Telefonie in vorhandene Sicherheitsstrukturen in Netzen einzubinden ist,
- welche Probleme bei VoIP über Vertrauensgrenzen hinweg entstehen und wie sie zu lösen sind,
- welche rechtlichen Aspekte bei VoIP-Sicherheit relevant sind.

Die Referenten blicken auf jahrelange Projekterfahrungen im Bereich VoIP und Informationssicherheit zurück und vermitteln diese Erfahrungen im Seminar.

Referent: Dr.-Ing. Behrooz Moayeri

Preis: € 1.390,- zzgl. MwSt.



Buchen Sie über unsere Web-Seite [www.comconsult-akademie.com](http://www.comconsult-akademie.com)

## Service Level - Steuerung der Leistungsqualität in der Praxis

Teil sogar über die Grenzen der IT hinaus. Beispiele können Sicherheitspolitik, Unternehmensgrundsätze, Festlegungen von Meldewegen für typische auslösende Ereignisse u.ä. sein.

Derartige Dokumente stellen verbindliche Rahmenbedingungen dar, die bei der Erbringung von IT-Services nicht diskutabel sind.

- IT-spezifische Festlegungen auf Prozessebene

Hier werden wichtige Hauptprozesse oder grundlegende Verfahrensweisen im IT-Bereich festgelegt, etwa Change Management im Zuständigkeitsbereich IT,

Grundkonzeption und zugehörige Abläufe zur Datensicherheit, Notfallkonzeption bzw. Notfallhandbuch IT usw. Diese können die IT als Ganzes oder einzelne Teilbereiche (Netzwerk, Systembetrieb, Endgerätebereich, ...) betreffen.

Wesentlich zur Abgrenzung der nachfolgend benannten Begriffe ist die Festlegung von Prozessen, d.h. insbesondere der Ablauforganisation mit Zuordnung von Zuständigkeiten, und dabei eine geringe Bindung an konkrete Produkte und Versionen. (s. Abb. 7)

- Anleitungen unter Produkt- und Versionsbezug

Je nach benötigtem Detaillierungsgrad

wird hier für derzeit eingesetzte Produkte und Produktversionen die Schrittabfolge für bestimmte typische Arbeitsgänge festgelegt, unter Benennung von Detailvorgaben für einzelne Schritte, sofern für einheitliche Ergebnisqualität notwendig.

Als Beispiel kann etwa der mit Kontrollfragenbeispiel 1. vorgeführte mögliche Installationswildwuchs im Endgerätebereich auf solche Weise bekämpft werden. Auf Basis eines grundlegend festgelegten Prozesses zur Endgeräteinstallation mit Prozess-Schritten „Vorbereitung, eigentliche Basisinstallation, Restinstallation (im Nutzerkontext etc.)“ kann diese im Spezialfall von Notebooks etwa wie in Abbildung 8 aussehen.

(wichtig: keine unnötigen Ausführungen zur Erläuterung, technische Grundlagen und Prozessverständnis beim Leser werden vorausgesetzt; Handzettel für die Durchführung durch geschultes und eingewiesenes Personal!)

- Checklisten

Hier handelt es sich um Laufzettel, die sowohl als Orientierungshilfe bei der einheitlichen Abarbeitung von Anleitungen gemäß vorigem Punkt genutzt werden können, als auch zugleich als Begleitdokumentation der Abarbeitung. Durch geschickte Vorbereitung der Inhalte kann sich die Dokumentationsarbeit zumeist auf Ankreuzen und Abzeichnen durch den Ausführenden beschränken. So können Einhaltung der Ablaufreihenfolge, Vollständigkeit der Abarbeitung und einheitliche Erfüllung von Nachweispflichten in einem gefördert werden, und dies bei minimalem Aufwand für den Durchführenden.

Anmerkung für die Praxis:

Dieses Art von Hilfsmittel kann begleitend nicht nur auf Ebene der Anleitungen, sondern auch auf Ebene übergeordneter Prozesse für typische Fälle eingesetzt werden, z.B. in Form eines Protokolltemplates für die Durchführung von Risikoanalysen im Rahmen des Change Management-Prozesses oder zur Erfüllung von entsprechenden Analyseaufträgen für besonders kritische IT-Lösungen.

Erzeugt man sich für alle relevanten IT-Lösungen derartige Hilfsmittel, so erfüllt man damit automatisch eine Vielzahl von Forderungen typischer Auflagen von außen,

| TABLE OF CONTENTS                           |     | Customer Logo |
|---------------------------------------------|-----|---------------|
| <b>1 Approval</b>                           | 4   |               |
| 1.1 Approval history                        | 4   |               |
| <b>2 Change History</b>                     | 5   |               |
| <b>3 Abstract</b>                           | 6   |               |
| 3.1 General Conditions                      | 6   |               |
| 3.2 The IT BPM                              | 7   |               |
| 3.3 Proceeding                              | 7   |               |
| 3.4 Scope of PROJECT                        | 8   |               |
| <b>4 Safeguarding Measures</b>              | 9   |               |
| 4.1 Summary of assigned measures            | 9   |               |
| 4.2 Interpretation of the charts            | 15  |               |
| 4.3 All IT Systems                          | 16  |               |
| 4.4 All Windows computers                   | 16  |               |
| 4.5 Windows Server                          | 43  |               |
| 4.6 Terminal Server                         | 56  |               |
| 4.7 TCP/IP                                  | 56  |               |
| 4.8 Active Directory                        | 60  |               |
| 4.9 Group Policies                          | 70  |               |
| 4.10 File and Print                         | 73  |               |
| 4.11 Windows Clients                        | 77  |               |
| 4.12 Exchange and Outlook                   | 104 |               |
| 4.13 Antivirus                              | 119 |               |
| 4.14 Firewall and Internet/Intranet Access  | 128 |               |
| 4.15 Migration                              | 128 |               |
| 4.16 Documentation Strategy                 | 133 |               |
| 4.17 Processes and Administration           | 137 |               |
| 4.18 User Handbook and Training             | 154 |               |
| <b>5 Glossary</b>                           | 162 |               |
| 5.1 Terms & Definitions                     | 162 |               |
| <b>6 Related Documents</b>                  | 162 |               |
| 6.1 Overview                                | 162 |               |
| <b>7 Index</b>                              | 162 |               |
| PROJECT - Technical Architecture - Security |     | 2             |

Abbildung 7: Beispielinhaltsverzeichnis IT-Sicherheitskonzept Client-Server-Infrastruktur

## Service Level - Steuerung der Leistungsqualität in der Praxis

## Anleitung zur Notebook-Installation auf Basis von Windows XP

## Inhaltsverzeichnis

|                                                                                    |   |
|------------------------------------------------------------------------------------|---|
| 1. Zweck .....                                                                     | 1 |
| 2. Geltungsbereich .....                                                           | 1 |
| 3. Beschreibung .....                                                              | 2 |
| 3.1 Vorbereitende Arbeiten .....                                                   | 2 |
| 3.1.1 Erfassen des Notebooks im Desktop Management .....                           | 2 |
| 3.1.2 Vorbereitung Betriebssystemergänzungen .....                                 | 2 |
| 3.1.3 Anbringen der Inventarnummer am Notebook .....                               | 2 |
| 3.1.4 BIOS-Einstellungen .....                                                     | 3 |
| 3.2 Eigentliche Basisinstallation .....                                            | 5 |
| 3.2.1 Installation von Image und Betriebssystemerweiterungen .....                 | 5 |
| 3.2.2 Installation nutzerbezogene Software .....                                   | 5 |
| 3.2.3 Funktionstest von Modem- oder ISDN-Hardware .....                            | 5 |
| 3.3 Restinstallation .....                                                         | 6 |
| 3.3.1 Zwischenspeicherung persönlicher Einstellungen auf ext. HDD [optional] ..... | 6 |
| 3.3.2 Synchronisierung PDA-relevanter Daten vom Alt-PC-Endgerät [optional] .....   | 7 |
| 3.3.3 Durchlaufen der Applikationsverarbeitung .....                               | 7 |
| 3.3.4 Übernahme persönlicher Einstellungen von Altgerät [optional] .....           | 7 |
| 3.3.5 Konfiguration von Notes, evtl. VPN und RAS-Client .....                      | 8 |

Abbildung 8: Beispiel Installationsanleitung für Standard-Notebooks

Dann werden in der Konfigurationsoberfläche für das BIOS die Einstellungen wie folgt modifiziert:

- Punkt Sicherheitsfunktionen - Gerätesicherheit:
  - Alle Einstellungen auf „Aktiviert“ setzen, insbesondere
  - InternerNetzwerkAdapter-Start
- Punkt Sicherheitsfunktionen:
  - Festgelegtes Administratorpasswort setzen
- Punkt Erweiterungen:
  - Sprache auf „Deutsch“ stellen
- Punkt Erweiterungen - Start-Optionen:
 

|                                            |           |
|--------------------------------------------|-----------|
| • Quickboot                                | Aktiviert |
| • Wartedauer für F10 und F12(s)            | Wert 0    |
| • Multiboot                                | Aktiviert |
| • Verzögerung für Express-Boot-Popup (sek) | Wert 0    |

Ansonsten ist die Startreihenfolge einzustellen:

- Startreihenfolge:
  - Festplatte Notebook 1

Abbildung 9: Detailvorgaben in Installationsanleitung Notebook - „BIOS-Einstellungen“

etwa der ISO 27001. Die vorgeschlagenen und beispielhaft dargestellten Hilfsmittel bilden zudem eine in sich schlüssige Hierarchie, die eine Durchgängigkeit der Umsetzung von Vorgaben/ Forderungen zur Service-Güte sicherstellen.

Außerdem erleichtern sie deutlich die Einhaltung solcher Vorgaben in der täglichen Praxis: ist eine funktionierende und vorschriftsmäßige Arbeitsweise einmal erarbeitet, per Tests verprobt und in entsprechenden Dokumenten festgehalten, kann sich der Durchführende auf die durch solche Hilfsmittel geführte Anwendung seines IT-Fachwissens konzentrieren. Auch dem Diszipliniertesten platzt irgendwann der Kopf, wenn er sowohl Produktwissen als auch ein komplexes Werk an Vorgaben in mehreren Hierarchiestufen auswendig beherrschen und jederzeit zielsicher anwenden soll. Auch das „Ausdenken“ geeigneter Formulierungen zur vorgesehenen Dokumentation entfällt oder wird auf ein Minimum reduziert (Bemerkungsfelder).

Der Vollständigkeit halber lässt sich vorführen, dass sich ein solcher Satz von „organisatorisch-technischen Hilfsmitteln“ mit der zuvor motivierten Technik der Verlinkung leicht zu typisch geforderten Gesamtdokumenten, etwa Betriebshandbüchern zusammenführen lässt. Wendet man wie im nachfolgenden Beispiel geschehen z.B. Web-Technik als Verlinkungsbasis an, erhält man neben einem „vorschriftsmäßigen“ Betriebshandbuch zugleich einen guten Navigationseinstieg zur schnellen Orientierung innerhalb des Gesamtvorrats solcher Hilfsmittel-Dokumente. (siehe Abbildung 11)

Abschließend eine letzte Anmerkung, ebenfalls begründet aus der ComConsult-Projektpraxis. Häufig wird versucht, den Aufwand der Erstellung entsprechender Hilfsmittel- und Vorgabedokumente und der damit verbundenen Konzeption von Prozessen und Arbeitsweisen vollständig

## Vorbereitende Arbeiten

|                                                                                                                                                            |                                                                                                                                 |
|------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| Erfassen des Notebooks im Desktop Management                                                                                                               | Erfassung erfolgt <input type="checkbox"/>                                                                                      |
| Vorbereitung Betriebssystemergänzung durch Zuweisung entsprechender automatischer Installation                                                             | Betriebssystemergänzung zugewiesen <input type="checkbox"/><br>Betriebssystemergänzung nicht notwendig <input type="checkbox"/> |
| Anbringen der Inventarnummer am Notebook<br>Prüfen, ob Inventarnummer zugewiesen; Nummer aus Auftrag entnehmen, Schild befestigen                          | Inventarnummer angebracht <input type="checkbox"/>                                                                              |
| BIOS-Einstellungen nach Vorgabe<br>Die BIOS-Einstellungen werden auf einen festgelegten, qualitätsgesicherten Stand gesetzt (siehe Installationsanleitung) | BIOS-Einstellungen nach Vorgabe vorgenommen <input type="checkbox"/>                                                            |

Abbildung 10: Checkliste zur Notebook-Installation

## Service Level - Steuerung der Leistungsqualität in der Praxis

abzuwälzen, indem eine IT-Dienstleistung pauschal als „Full Service“ eingekauft bzw. als Benchmarking-Basis abgefragt wird.

Es ist aber ein trügerischer Gedanke, dass man auf diesem Wege aus dem Schneider sei. Der Aspekt der Vergleichbarkeit wurde zuvor schon beleuchtet, mindestens hier ist ein schwerwiegendes Argument gegeben, dennoch bis zu einem gewissen Grad verbindliche Vorgaben zu machen.

Wer sich der kritischen Begutachtung durch unabhängige Dritte (interne Revision oder externes Audit, etwa zur Zertifizierung oder zur Prüfung der Einhaltung von

Vorgaben aus Quellen wie FDA, BaFin, ...) stellen muss, kann den Aufwand nur bedingt per outsourcing „loswerden“. Selbst wenn ein Externer entsprechend zertifiziert ist, stellt dies keine rundum sorglos-Garantie dar! Beispiel: eine Zertifizierung nach BS 7799-2 oder zukünftig ISO 27001 sichert zunächst nur einen Prozess, der ein vorgegebenes Niveau der Informationssicherheit aufrechterhält. Die Gestaltung dieses Prozesses sowie die Führung des Nachweises seiner praktischen Umsetzung kann man auf den Externen verlagern, und die Kontrolle über Forderung entsprechender Zertifizierung vereinfachen. Dennoch muss man eine Mindestkontrolle und -Steuerung ausüben:

nämlich durch Definition von Richtwerten, etwa einzuhaltenden technischen Konzepten oder Detailvorgaben für besonders kritische Systeme etc. Aktuelle Versionen entsprechender Vorgaben, etwa aus 2005 stammende Versionen entsprechender ISO-Standards, tragen dem Rechnung, indem gezielt zusätzliche „Controls“ zum steuernden Umgang mit Externen aufgenommen wurden. Die Gefahr der „leichtfertigen“ Abwälzung der Gestaltungs- und Steuerungsaufgabe ist also erkannt - man wird sich auf Dauer einer Mindestarbeit im Sinne des soeben Gelesenen nicht entziehen können.

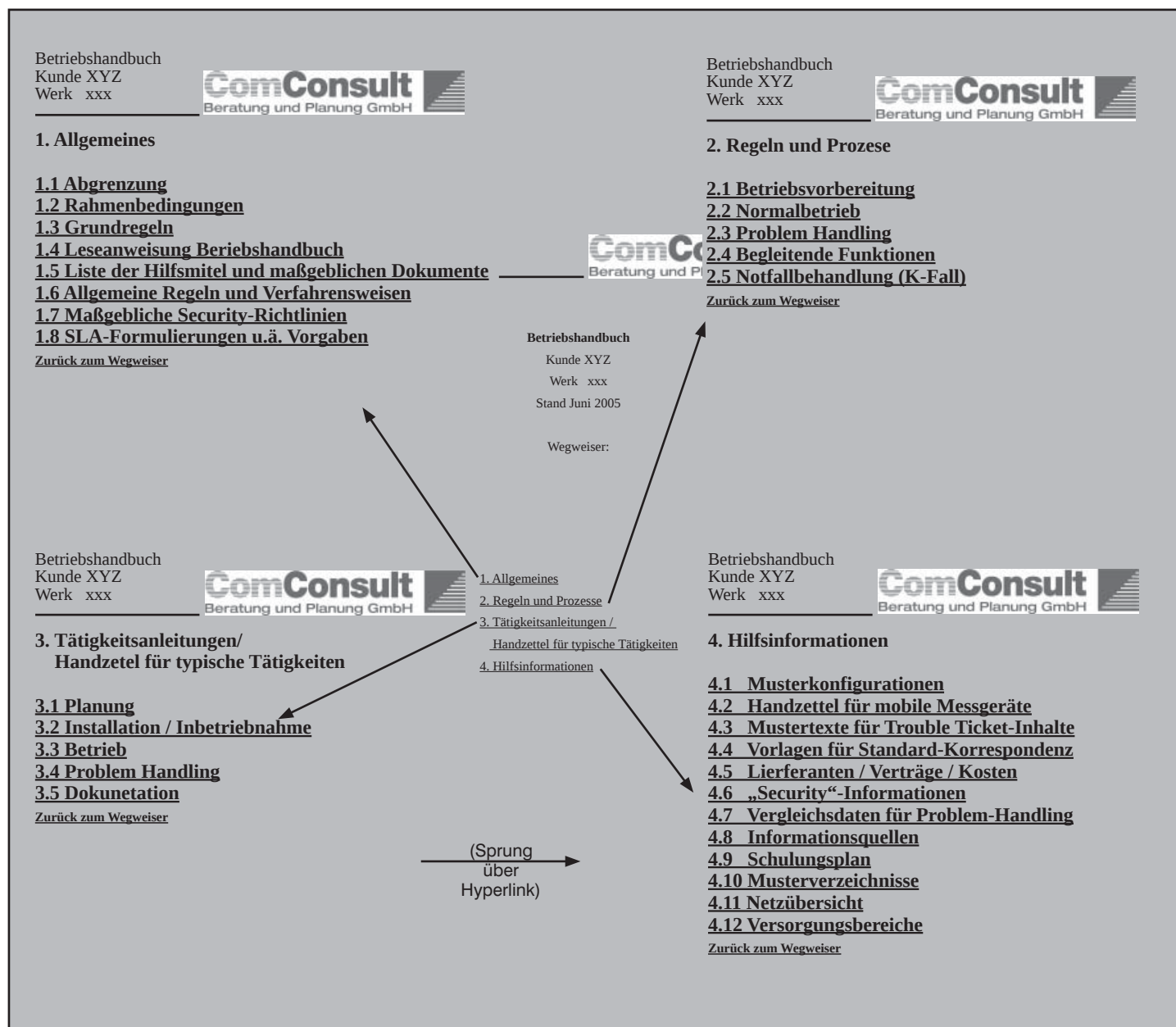


Abbildung 11: Beispiel Bildung eines Betriebshandbuchs durch Verlinkung verschiedener Dokumente

# Aktuelle Veranstaltungen

**Sicherheit im Netzwerk: Trennung von Benutzergruppen und Zugriffsschutz auf Benutzer-Ebene, 25.09. - 27.09.06 in Neuss**

Dieses Seminar richtet sich an Planer und Betreiber von Netzwerken mit einer Zentralen Authentifizierung. Weitere Schwerpunkte sind die Einräumung von Zugangsrechten, die Überprüfung von Patchleveln vor dem Netzwerk-Access und die Überwachung des Netzes auf abnormales Verhalten.

Preis: € 1.690,- zzgl. MwSt.

**Troubleshooting Windows Server 2003 Active Directory, 25.09. - 28.09.06 in Aachen**

Dieses 4-tägige Seminar besteht aus einem Mix aus Know-How-Auffrischungen, Aufgaben, Live-Demonstrationen und Troubleshooting durch die Teilnehmer selber, so dass ein hoher Praxisgrad erreicht wird. Die Referenten kommen vom bekannten Competence Center Backoffice der ComConsult Beratung und Planung, das auf zahlreiche erfolgreiche nationale und internationale AD-Projekte im Bereich von ca. 300 bis zu 80.000 Benutzer/Computer zurück blicken kann.

Preis: € 1.990,- zzgl. MwSt.

**Sicherheit 2: VPN Virtuelle Private Netze: Planung, Konfiguration, Betrieb, 25.09. - 27.09.06 in Neuss**

VPN-Technologie ist ein unverzichtbarer Teil jeder Netzwerk-Sicherheits-Lösung. Ebenso vielfältig wie die Nutzungsformen sind die Realisierungs-Alternativen und die Integration in bestehende Netzwerk-Infrastrukturen. Dieses 3-tägige Seminar bewertet die bestehenden Alternativen und gibt direkt in der Praxis umsetzbare Empfehlungen zur optimalen Nutzung von VPN-Technologien.

Preis: € 1.690,- zzgl. MwSt.

**Ethernet Technologien neuester Stand, 25.09. - 29.09.06 in Aachen**

Dieses Seminar stellt die neuesten Ethernet- und Wireless-Varianten vor und zeigt, nach welchen Regeln und Auslegungsvorschriften diese zu konfigurieren sind. Mit besonderem Blick auf die Praxis werden Komponenten- und Kabeltechnik erläutert, auch wichtige Betriebsfragen werden vorgestellt. Im Besonderen wird die Bedeutung der IP-Telefonie für die Gestaltung von Ethernet-LANs analysiert. Abgerundet wird das Seminar um wichtige Fragen des Trouble-Shootings.

Preis: € 2.290,- zzgl. MwSt.

**TCP/IP und SNMP, 25.09. - 29.09.06 in Neuss**

Dieses 5-tägige Seminar vermittelt systematisch die Grundlagen TCP/IP, beleuchtet Vor- und Nachteile und gibt wichtige Empfehlungen für den erfolgreichen Einsatz. Dies betrifft speziell auch die wichtigen IP-Infrastrukturdienste von der Adressierung über ARP bis zu DHCP, DNS, DDNS und NAT und die Management-Funktionalität SNMP.

Preis: € 2.290,- zzgl. MwSt.

**EMV-gerechte Planung der Elektroinstallation für Rechnerräume und Rechenzentren, 25.09. - 26.09.06 in Berlin**

Dieses Seminar zeigt, wie eine EMV-gerechte, hochverfügbare und störungsarme Elektroinstallation mit gleichzeitig hoher Betriebssicherheit geschaffen werden kann. Es vermittelt mit engem Bezug zur Praxis wie ausgehend von Analyse und Messtechnik bestehenden Mängel beseitigt werden und ein wartungsoptimierter Betrieb aufgebaut wird.

Preis: € 1.390,- zzgl. MwSt.

**Troubleshooting Exchange Server 2003, 16.10. - 17.10.06 in Aachen**

Dieses 2-tägige Seminar ruft bewährte Technologien der Exchange Server-Produkte nochmals bei den Teilnehmern in Erinnerung und zeigt anhand dieses Know-How effiziente Maßnahmen zur Sicherung, Reparatur und Wiederherstellung von Exchange-Daten auf. Des Weiteren werden die Möglichkeiten betrachtet, die Exchange Server 2003 mit integriertem Service Pack 2 bietet, um dem wachsenden Problem zu begegnen, welches durch die Flut unerwünschter Nachrichten entsteht.

Preis: € 1.390,- zzgl. MwSt.

**Trouble Shooting für TCP/IP- und Windows-Umgebungen, 16.10. - 20.10.06 in Aachen**

Dieses Seminar beschreibt die typischen Störsituationen in diesem Umfeld, 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.

Preis: € 2.490,- zzgl. MwSt.

**Quality of Service, 16.10. - 17.10.06 in Köln**

Dieses 2-tägige Seminar befasst sich mit Quality of Service (QoS) in LAN, WAN und WLAN. Sie lernen, wann QoS erforderlich ist, welche QoS-Standards es gibt, wie eine beherrschbare Architektur aussieht und wie QoS funktioniert.

Preis: € 1.390,- zzgl. MwSt.

**Session Initiation Protocol SIP - Basis-Technologie der IP-Telefonie, 16.10. - 18.10.06 in Köln**

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.

**Sicherheitsmechanismen für Voice over IP, 19.10. - 20.10.06 in Köln**

Angesichts der Offenheit und geringeren Verfügbarkeit von Datennetzen ist das Thema Sicherheit das zentrale Projektthema bei der Umsetzung von Voice over IP. VoIP benötigt Sicherheitsmechanismen, die mindestens ein den konventionellen Telekommunikationsnetzen entsprechendes Niveau an Vertraulichkeit, Verlässlichkeit, Verfügbarkeit und Integrität sicherstellen. Darüber hinaus bietet die Umstellung die Chance, die Sicherheit der Sprachkommunikation über das bisherige Niveau hinaus zu verbessern.

Preis: € 1.390,- zzgl. MwSt.

## CCNE

### ComConsult Certified Network Engineer

#### Lokale Netze

23.10. - 27.10.06 in Neuss  
04.12. - 08.12.06 in Aachen  
05.02. - 09.02.07 in Aachen  
16.04. - 20.04.07 in Aachen  
25.06. - 29.06.07 in Aachen  
15.10. - 19.10.07 in Aachen  
03.12. - 07.12.07 in Aachen

#### Internetworking

11.09. - 15.09.06 in Aachen  
13.11. - 17.11.06 in Aachen  
05.03. - 09.03.07 in Aachen  
07.05. - 11.05.07 in Aachen  
17.09. - 21.09.07 in Aachen  
10.12. - 14.12.07 in Aachen

#### TCP/IP und SNMP

25.09. - 29.09.06 in Köln  
27.11. - 01.12.06 in Berlin  
26.02. - 02.03.07 in Berlin  
21.05. - 25.05.07 in Aachen  
17.09. - 21.09.07 in Neuss  
19.11. - 23.11.07 in München

#### Ethernet Technologien - neuester Stand

25.09. - 29.09.06 in Aachen  
27.11. - 01.12.06 in Aachen  
26.02. - 02.03.07 in Aachen  
21.05. - 25.05.07 in Aachen  
10.09. - 14.09.07 in Aachen  
26.11. - 30.11.07 in Aachen

Paketpreis für alle vier Seminare € 8.244.-- zzgl. MwSt.  
(Einzelpreise: je € 2.290.--)



Buchen Sie über unsere Web-Seite  
[www.comconsult-akademie.com](http://www.comconsult-akademie.com)

## CCTS

### ComConsult Certified Trouble Shooter

#### Trouble Shooting in Lokalen Netzwerken - Grundlagen

04.09. - 08.09.06 in Aachen  
06.11. - 10.11.06 in Aachen  
12.03. - 16.03.07 in Aachen  
11.06. - 15.06.07 in Aachen  
03.09. - 07.09.07 in Aachen  
12.11. - 16.11.07 in Aachen

#### Trouble Shooting in konvergenten Netzwerken

18.09. - 22.09.06 in Aachen  
13.11. - 17.11.06 in Aachen  
23.04. - 27.04.07 in Aachen  
18.06. - 22.06.07 in Aachen  
17.09. - 21.09.07 in Aachen  
19.11. - 23.11.07 in Aachen

#### Trouble Shooting für TCP/IP- und Windows-Umgebungen

16.10. - 20.10.06 in Aachen  
29.01. - 02.02.07 in Aachen  
07.05. - 11.05.07 in Aachen  
22.10. - 26.10.07 in Aachen

Paketpreis für alle drei Seminare, eine digitale Stromzange, die Prüfung und den Report „Fehlersuche in konvergenten Netzen“ € 6.990.-- zzgl. MwSt.  
(Einzelpreise: je € 2.490.--)



Buchen Sie über unsere Web-Seite  
[www.comconsult-akademie.com](http://www.comconsult-akademie.com)

## CCSE

### ComConsult Certified Security Expert

#### Sicherheit 1: Kernbausteine einer erfolgreichen Sicherheits-Lösung

11.09. - 15.09.06 in Bonn  
12.02. - 16.02.07 in Aachen  
18.06. - 22.06.07 in Bonn  
10.09. - 14.09.07 in Berlin

#### Sicherheit 2: VPN Virtuelle Private Netze: Planung, Konfiguration, Betrieb

25.09. - 27.09.06 in Köln  
05.03. - 07.03.07 in Bonn  
25.06. - 27.06.07 in Berlin  
15.10. - 17.10.07 in Aachen

#### Sicherheit 3: Praxis-Intensiv-Seminar zur erfolgreichen Konfiguration von Firewall, VPN, Windows-Clients, WLANs

23.10. - 27.10.06 in Aachen  
16.04. - 20.04.07 in Aachen  
27.08. - 31.08.07 in Aachen  
03.12. - 07.12.07 in Aachen

Paketpreis für alle drei Seminare und Report „VPN-Technologien: Alternativen und Bausteine einer erfolgreichen Lösung“ € 5.990.-- zzgl. MwSt. (Einzelpreise: € 2.290.-- / € 1.690.-- / € 2.290.-- / Report 398.--)



Buchen Sie über unsere Web-Seite  
[www.comconsult-akademie.com](http://www.comconsult-akademie.com)

## Impressum

Verlag:  
ComConsult Technology Information Ltd.  
121 Paton Rd.  
RD1  
Richmond  
New Zealand  
GST Number 84-302-181  
Registration number 1260709  
Phone: 0064 3 5444632  
Fax: 0064 3 5444237

German Hot-line of ComConsult-Research: 02408-955300  
E-Mail: [insider@comconsult-akademie.de](mailto:insider@comconsult-akademie.de)  
<http://www.comconsult-research.de>

Herausgeber und verantwortlich im Sinne des Presserechts:  
Dr. Jürgen Suppan  
Chefredakteur: Dr. Jürgen Suppan  
Erscheinungsweise: Monatlich, 12 Ausgaben im Jahr  
Bezug: Kostenlos als PDF-Datei  
über den eMail-VIP-Service der ComConsult Akademie

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