

Schwerpunktthema

# Troubleshooting Windows Server 2003 Active Directory – oft eine komplexe Sache!

von Markus Holländer

Mit der Version 2 des Active Directory, die ja mit Windows Server 2003 auf dem Markt kam, hat Microsoft seinen Verzeichnisdienst weiter verbessert. Dies ändert jedoch nichts an der Komplexität und den vielfältigen Möglichkeiten, die die Implementierung und der Betrieb mit sich bringen.

Dieser Artikel erläutert einige „kleinere Troubles“, die man mit dem Active Directory haben kann. Ich selber habe schon verschiedenste Implementierungen vorangetrieben und/oder betreut, sei es in nationalen oder internationalen Projekten von einigen hundert bis hin zu mehreren zehntausend Rechnern bzw. Userobjek-



ten. Vorweg sei jedoch angemerkt, dass man sagen kann, dass das Active Directory schon oft sehr leidensfähig ist, bevor es richtig Ärger macht. Dies haben all diese Projekte gezeigt. Und noch ein weiterer Punkt am Anfang: Wenn man elementare Probleme mit dem Active Directory hat, sollte man als erstes an das IP-Management (DNS, NetBIOS) denken, hier liegt dann die Lösung für ein Großteil der Probleme, ich selber schätzen den Anteil auf 80%.

weiter auf Seite 21

Zweitthema

## Business Continuity Planning

von Holm Diening

Die IT-Infrastruktur ist mittlerweile vitaler Bestandteil der Geschäftsprozesse fast jeden Unternehmens. Aus diesem Grunde kann ihr Versagen auch schwerste Schäden sogar bis hin zum Konkurs verursachen. Maßnahmen zur Notfallplanung werden deshalb zuneh-

mend wichtiger und unterstützen die Aufrechterhaltung des Geschäftsbetriebes nach einem Schadensfall.

Dieser Artikel gibt zunächst eine Einführung in die Thematik und beschreibt dann die wesentlichen Phasen des Business

Continuity Planning für den IT-Bereich. Dabei geht er auch auf Aspekte der praktischen Umsetzung und den Einsatz von Softwaretools zur Unterstützung ein.

weiter auf Seite 9

Top Veranstaltung

### Gefahrenmelde- technik und Ob- jektüberwachung im Netz 2006

auf Seite 7

Zum Geleit

### Mobile Anwender im Visier der Hersteller

auf Seite 2

Report des Monats

### Sicherheit in Enterprise-Netzen durch den Einsatz von 802.1X

auf Seite 17

Zum Geleit

# Mobile Anwender im Visier der Hersteller

Mobile Anwender repräsentieren einen der attraktivsten Zukunftsmärkte. Ist ihr Zugang zu Unternehmensdaten bisher auf verschiedene Geräte, unterschiedlichste Oberflächen und ortsabhängige Zugangssysteme verteilt, so soll sich das in Zukunft ändern.

Ziel ist, dass jeder Mitarbeiter an Kernprozessen und Abläufen eines Unternehmens unabhängig

- vom Ort
- von der jeweiligen Zeitzone und der dort gegebenen Uhrzeit
- vom vorhandenen Endgerät teilnehmen kann.

Dies beinhaltet:

- die Kommunikation mit Sprache und Video
- den Zugang zu Daten
- den Zugang zu Applikationen

Im Endeffekt wird dies bedeuten, dass ein alles umfassender Client entsteht, der diese Gebiete abdeckt. Typische Projekte, die sich mit dieser Entwicklung befassen, sind:

- die Einführung von IP-Telefonie
- die Einführung von Kollaborations-Systemen
- die Neugestaltung der Unternehmens-Applikationen
- die Neuordnung des Zugangs zu Dokumenten

Leider ist der Aufbau einer derartigen Lösung nicht trivial. Jeder, der sich damit befasst, wird schnell feststellen, dass zwar alle wesentlichen Hersteller diese Entwicklung in den Mittelpunkt ihrer strategischen Entwicklungen gestellt haben, aber leider die damit entstehenden Produkte nicht auf einer technischen Linie liegen. Aus diesem Grund sind wichtige Produkt- und Herstellerentscheidungen zu einem sehr frühen Zeitpunkt zu treffen. Der Blick muss dabei auf den angestrebten Endausbau gelegt werden, sonst besteht die Gefahr von relativ teuren und arbeitsintensiven Sackgassen.

Die Strategien der Hersteller und die damit verbundenen Problematik der Findung einer einheitlichen Linie soll im folgenden an Beispielen verdeutlicht werden:

- ohne Frage ist Microsoft einer der Hersteller, denen eine Schlüsselrolle in der Umsetzung von Kollaborations-Clients in Zukunft zukommt.



Microsoft betreibt einen ganzen Warenkorb in diesem Funktionsbereich. Dazu gehören der Live Communication Server mit dem zugehörigen Client, die Sharepoint Services, der Messenger und das von Groove übernommene Virtual Office. Parallel wird in Windows Vista die Integration von mobilen Endgeräten, die auf Mobile Windows basieren, weiter ausgebaut. Spannend wird der Funktionsmix, der aus Sharepoint Version III in Kombination mit Groove entsteht. Voraussichtlich wird Groove als Teil von Microsoft Office 12 den Offline-Client realisieren, der den Zugang auf eine definierte Menge von Projekt-Ordern mit den zugehörigen Projekt-Planungsdaten ermöglicht. Für den Online-Betrieb wird der Zugang zu zentralen Ordnern und Dateien auf der Basis eines Sharepoint Portals in das neue Office 12 integriert, so dass hier zum Beispiel ein Zugriffssemaphor realisiert wird, der den schreibenden Zugriff auf eine in Benutzung befindliche Datei blockiert.

Einige Punkte bleiben in der Microsoft-Strategie unklar:

- Der genaue Funktionsumfang von Sharepoint III ist bisher nicht verbindlich festgelegt
- Das Zusammenspiel aus Groove und Office ist unklar, überhaupt gibt es keine Informationen zum nächsten Release des aktuellen Groove-Clients
- Microsoft versucht sich mit dem

Sharepoint-Portal in den Markt der Web-Server-Applikationen zu bewegen. Dieser wird bisher im Enterprise-Markt von IBM dominiert. Bisher muten die Versuche von Microsoft, hier einen Gegenpol aufzubauen mehr wie der Kampf David gegen Goliath an

- Die bisher öffentlich vorgeführten neuen Funktionalitäten erweckten bisher den Eindruck eines nicht abgestimmten und nicht zu Ende entwickelten Baukastens. Bevor nicht die neuen Versionen auf dem Markt sind, wird hier kaum Gewissheit über die Nutzbarkeit existieren. Nach der Verschiebung von Windows Vista und Office auf den Beginn von 2007 muss man befürchten, dass es noch eine Weile dauern wird bis hier Klarheit herrscht.

Unter dem Strich darf aber nicht unterschätzt werden, dass Microsoft im Besitz des Clients in den meisten Unternehmen ist. Der Ausbau der kombinierten Funktionalität aus Vista und Mobile Windows macht Microsoft zudem zu einem Major-Player im Markt für mobile Anwendungen

- Der direkte Konkurrent zu Microsoft ist IBM. Ist Microsoft im Besitz des Clients, so ist IBM im Besitz des Servers. Der sehr frühe und engagierte Einstieg in Web-Technologien hat IBM eine fast monopolartige Position verschafft. Aktuell drückt IBM massiv auf den Markt für Kollaborations-Clients und kommt damit in den direkten Wettbewerb zu Microsoft. Für die großen Unternehmen wird diese Konkurrenzsituation sicher zu den spannendsten Auseinandersetzungen der nächsten Jahre führen
- Den Gegenpol bildet das Lager der Kommunikationsfirmen wie Alcatel, Cisco und Siemens. Diese legen ihren funktionalen Schwerpunkt bisher auf Sprach- und Video-Kommunikation. Zwar gibt es immer wieder Ansätze, auch erweiterte Kollaborations-Funktionen aufzunehmen (OpenScape als Beispiel), doch der Fokus bleibt klar auf der Ebene der Kommunikation. Dies erzwingt fast natürlich die Notwendigkeit von strategischen Allianzen. Naturgemäß müssen dabei Microsoft und IBM im Mittelpunkt der Zusammenarbeit stehen. Ist dies bei IBM auch weitest-

## Mobile Anwender im Visir der Hersteller

gehend unkritisch, so ist jede Zusammenarbeit mit Microsoft ein zweischneidiges Schwert. Microsoft hat bereits mehrfach angedeutet, dass man eine eigene Sprachkommunikations-Lösung anstrebt. Die architektonische Betonung eines Präsenz-Servers und der Ausbau des Messengers zu einem immer mächtigeren Client unterstreichen das. In der Zusammenarbeit bzw. Abgrenzung zwischen Microsoft und den Kommunikationsanbietern liegt eines der großen Entscheidungsprobleme für alle betroffenen Anwender. Auf welches Pferd soll man hier setzen?

Nun könnte man sich ja gelassen im Sessel zurücklehnen und das Schauspiel des Wettbewerbs zwischen den genannten Firmen beobachten. Doch leider hat die sich hier andeutende Entwicklung Einfluss auf aktuelle Investitionsentscheidungen. Dies sein an Beispielen erläutert:

- Eine Kernfrage betrifft den mobilen Client der Zukunft. Welcher wird dies sein? Ist es das erweiterte Handy, der GSM-fähige PDA mit Windows Mobile oder ein Ultra-Kompakt-PC wie gerade auf der CeBIT vorgestellt? Wie auch immer, für die Unternehmen besteht der Zwang, den zurzeit gegebenen Wildwuchs zu beenden. Sobald der Zugang zu Unternehmensdaten erfolgt, müssen mobile Endgeräte einem zentralen Betrieb unterworfen werden, der die Installation aktuell hält und für aktuelle Sicherheitssysteme sorgt. Es ist offensichtlich, dass dies nicht für eine beliebige Menge von mobilen Clients machbar ist
- Das bisherige Telefon wird durch einen wesentlich weiter gehenden Kollaborations-Client abgelöst. Welcher Anbieter hat hier die Nase vorn? Und was bedeutet das für die Auswahl des Endgeräts? Soll hier mehr auf den Softclient gesetzt werden oder mehr auf das Hardphone? Und wie kann hier Funktionsgleichstand mit dem mobilen Endgerät erreicht werden?
- Der Funktionsumfang der modernen Kollaborations-Clients überdeckt sich immer mehr mit anderen IT-Bereichen. Beispiele sind Dokumenten-Management und Projekt-Management-Systeme. Hier ist ein klares Design und eine Aufteilung der Zuständigkeit erforderlich
- Mit dem Einstieg von Cisco auf der CeBIT in den Markt der Präsenz-Kommunikation wird der Druck auf dieses Thema erhöht. Nach Siemens, Alcatel und

Cisco ist somit ein weiterer großer Anbieter auf diesen Zug aufgesprungen. Gerade auch die Keynote von Chambers auf der VoiceCon unterstreicht das Bekenntnis von Cisco zu diesem Funktionsbereich. Bei näherer Betrachtung ist aber Sinn und Zweck von Präsenz-Kommunikation durchaus nebulös. Das ganze Thema scheint doch sehr auf die Vergangenheit ausgerichtet zu sein. Welchen Sinn macht Präsenzkommunikation, wenn die Erreichbarkeit eines Teilnehmers über einen mobilen IP-Client sowieso gewährleistet ist, dies ist doch gerade einer der Kern-Mehrwerte Umstellung von traditioneller TK auf Voice-over-IP, oder? Im Endeffekt reduziert sich die ganze Funktionalität einer Präsenz-Kommunikation dann auf die Pflege eines Benutzer-definierten Erreichbarkeits-Status, der ggf. für verschiedene Kontakte verschieden definiert werden kann. Dies rechtfertigt aber auf keinen Fall die bisher von den Herstellern angebotenen sehr komplexen Architekturen Investitionskosten und Betriebsaufwände.

Betrachtet man die zuvor genannten Beispiele, dann wird deutlich, dass hier Handlungsbedarf besteht. Es muss vermieden werden, dass über den vorschnellen Einstieg in Einzeltechnologien frühe Entscheidungen getroffen werden, die im

Sinne der zu schaffenden Gesamtfunktionalität in eine Sackgasse führen.

Mehr denn je besteht die Notwendigkeit zur Festlegung der folgenden Entscheidungen:

- wie sieht die mobile Kommunikation im Unternehmen in Zukunft aus?
- welche Funktionalitäten soll sie umfassen?
- welches mobile Endgerät soll eingesetzt werden?
- wie ist das Zusammenspiel Sprache-Video-Daten-Applikation?
- welches Sicherheitssystem ist erforderlich?
- wie sieht der Betrieb für die Gesamtlösung aus?
- wer ist für diese Art von Kommunikation im Unternehmen überhaupt zuständig?

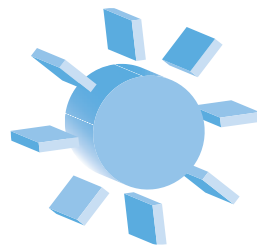
Werden diese Fragen nicht sauber geregelt, werden funktionale Inseln entstehen, die den angestrebten und auch erreichbaren Mehrwert in Frage stellen.

Wir helfen Ihnen auf diesem Weg. Sowohl in der Sommerschule 2006 als auch in unserem Spezialseminar zur Mobilkommunikation greifen wir dieses Thema auf.

Ihr

Dr. Jürgen Suppan

## Sommerschule 2006



**19.06. - 23.06.06  
in Aachen**

Die Sommerschule 2006 greift die aktuellsten Entwicklungen der Netzwerk-Technologien auf, stellt die wichtigsten Trends zur Diskussion und gibt Empfehlungen zur Weiterentwicklung und Verbesserung bestehender Netzwerke. Mit diesem 5-Tages-Intensiv-Update auf den letzten Stand der Netzwerk-Technik haben wir für Sie die aktuellen Entwicklungen analysiert, Erfahrungen aus Labor und gerade abgeschlossenen Projekten eingearbeitet und daraus eine Auswahl aus den zur Zeit anliegenden Top-Themen getroffen.

Preis: € 1.990,-\* zzgl. MwSt. (\*gültig bis 15.05.06 - dann regulär € 2.290,- zzgl. MwSt.)



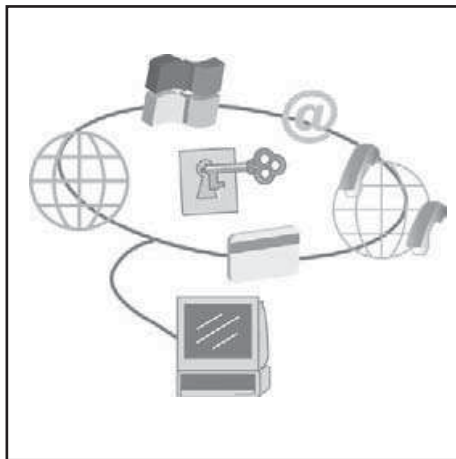
Buchen Sie über unsere Web-Seite [www.comconsult-akademie.com](http://www.comconsult-akademie.com)

IT-Sicherheits-Kongress

# IT-Sicherheits-Forum 2006

Die Comconsult Akademie veranstaltet zusammen mit der GAI NetConsult Berlin vom 08. - 11. Mai das „IT-Sicherheits-Forum 2006“ in Bad Neuenahr.

Das IT-Sicherheits-Forum 2006 wird auch in diesem Jahr wieder die gerade aktuellen Themen zu Bedrohungsszenarien der IT-Sicherheit und zu den wichtigsten Schutzmaßnahmen aufgreifen. Dabei wird ein äußerst großer Wert auf Praxisnähe gelegt, dies zeigt sich insbesondere bei den technisch orientierten Workshops und den Praxisvorträgen, die direkt anwendbare „Tipps & Tricks“ für den Tagesbetrieb weitergeben. Das Forum hat sich deshalb in den letzten Jahren zu einem stark besuchten Treffpunkt für alle Sicherheitsinteressierten entwickelt. An insgesamt vier Tagen werden angeboten:



- Erfahrungen aus aktuellen Sicherheitsvorfällen und Aufzeigen absehbarer Trends
- Neue Entwicklungen bei Sicherheitstechnologie und Sicherheitsorganisation
- Moderierte Workshops mit Produktvergleichen und Live-Demos
- Vertiefende Seminare und Tutorien

Der (optionale) 1. Tag hat einführenden Charakter mit insgesamt drei parallelen Seminaren. Am 2. und 4. Tag werden durch erfahrene Referenten aktuelle Fachthemen analysiert und Praxiszenarien vorgestellt. Der 3. Tag ist mehreren Workshops für Produktvergleiche und Fallstudien zu aktuellen Sicherheitsthemen vorbehalten. Da diese parallel ablaufen, kann jeder Teilnehmer das für ihn optimale Programm selber zusammenstellen.

Fax-Antwort an ComConsult 02408/955-399

## Anmeldung IT-Sicherheits-Forum 2006

Ich buche den Kongress **IT-Sicherheits-Forum 2006** vom 08.05. - 11.05.06 in Bad Neuenahr

**mit Tutorium am ersten Tag**

- Thema 1    Thema 2    Thema 3

zum Preis von nur € 2.190,- zzgl. MwSt.

- ohne Tutorium am ersten Tag

zum Preis von nur € 1.790,- zzgl. MwSt.

**Workshopauswahl am 10.05.06**

**vormittags**

- Workshop 1  
 Workshop 2  
 Workshop 3  
 Workshop 4

**nachmittags**

- Workshop 3  
 Workshop 5  
 Workshop 6  
 Workshop 7

**mit Report**

„Sicherheit in Enterprise-Netzen durch den Einsatz von 802.1X“

zum Preis von nur € 338,- zzgl. MwSt.

- ohne Report**

- Bitte reservieren Sie für mich ein Hotelzimmer

vom \_\_\_\_\_ bis \_\_\_\_\_ 06

\_\_\_\_\_  
Vorname

\_\_\_\_\_  
Nachname

\_\_\_\_\_  
Firma

\_\_\_\_\_  
Abteilung

\_\_\_\_\_  
Telefon

\_\_\_\_\_  
Fax

\_\_\_\_\_  
Straße

\_\_\_\_\_  
PLZ, Ort

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

\_\_\_\_\_  
eMail

\_\_\_\_\_  
Unterschrift

## Programmübersicht IT-Sicherheits-Forum 2006

**Montag, 08.05.06 Tutorien**

**Alle Tutorien finden parallel statt und starten um 10:00 Uhr und enden gegen 17:30 Uhr.  
Bitte wählen Sie Ihr bevorzugtes Tutorium aus (Anmeldung)**

**Tutorium 1: Aktuelle Themen der IT-Security - Angriffe, Konzepte, Lösungen im Überblick (mit Live-Demo)**

- **Vorstellung realer Angriffsszenarien**
- **Grundlagen der IT-Sicherheit**  
Umgang mit Risiken, Schutzziele, Elementare Maßnahmen  
Security Policy, Grundschutz, BS 7799
- **Grundlagen der Verschlüsselungstechnologie**  
Einführung, Kryptografie, aktuelle Standards
- **Lösungen zur E-Mail Sicherheit**  
Client-Plug-Ins, Gatewaylösungen
- **Von Firewall bis VPN**  
Konzepte, DMZ, Betrieb, Praxis
- **Sicherheitsfunktionen von Windows 2003/XP**  
Distributed Security Services, SmartCards
- **Sichere Server**  
Logging, Backup, Hardening  
*Hans-Joachim Knobloch,  
Secorvo Security Consulting GmbH*

**Tutorium 2: VoIP-Security Technische und Rechtliche Sicherheit (mit Live-Demo von Angriffen)**

- **Kurzvorstellung VoIP**
- **Gefahren bei der Nutzung von VoIP**  
Angriffe gegen VoIP-Kommunikation  
Bedrohungen durch Verwendung dynamischer Ports  
Transport von Malware über VoIP-Protokolle
- **Angriffe auf Handy- und WLAN-Funkstrecken**
- **Rechtliche Sicherheit bei VoIP**  
Fernmeldegeheimnis und Betriebsverfassungsrecht
- **Sicherheitsanforderungen an VoIP**

*Ulrich Emmert, Frank Gebert  
esb Rechtsanwälte*

**Tutorium 3: Layer-2 Security - Angriffe gegen die Netzwerk-Infrastruktur (mit Live-Demo von Angriffen und Tools)**

- **Überblick zu Layer-2 Technologien und Protokollen**
- **Vorstellung der wichtigsten Sicherheitsprobleme**
- **Layer-2 Security Features (Private VLANs, DHCP Snooping, ARP Inspection, 802.1X)**
- **Ausblick auf moderne WAN-Technologien (Metro Ethernet, Ethernet over MPLS, Virtual Private LAN Services)**
- **Auswirkungen auf die Layer-2 Security**

*Enno Rey  
ERNW Netzwerke GmbH*

**11:30 - 12:00 Uhr Kaffeepause  
13:00 - 14:30 Uhr Mittagspause  
16:00 - 16:30 Uhr Kaffeepause**

**Dienstag, 09.05.06**

**10:00 Uhr – 10:15 Uhr  
Begrüßung/Übersicht**

*Detlef Weidenhammer,  
GAI NetConsult GmbH*

**10:15 Uhr – 11:00 Uhr**

**Sicherer Umgang mit modernen Kommunikationsformen**

- Instant Messaging: Von ICQ bis Jabber - Nutzen oder verbieten?
- Peer-to-Peer: von eDonkey bis Bittorent - was geht davon im Unternehmen?
- Anonymisierungsdienste im Unternehmen: Datenschutz gegen IT-Sicherheit?
- Von http-Tunnel bis JAP: Warum überhaupt noch eine Firewall?

*Prof. Dr. Rainer W. Gerling  
Max-Planck-Gesellschaft*

**11:00 Uhr – 11:45 Uhr**

**Zunehmende Kriminalisierung des Internet**

- Massenhaft vorgetragene Angriffe (Phishing, Botnets usw.)
- Gezielte Angriffe mit Spyware
- Attacken auf kritische Infrastrukturen
- Abwehrmaßnahmen

*Detlef Weidenhammer,  
GAI NetConsult GmbH*

**12:15 Uhr – 13:00 Uhr**

**IT-Sicherheit in kritischen Infrastrukturen**

- Einführung in die Thematik „Kritische Infrastrukturen“
- Nationale und internationale Aktivitäten
- KRITIS-Materialien des BSI
- Sicherheitsrichtlinie und -check in der Praxis

*Stefan Gunzelmann,  
consequa GmbH*

**14:30 Uhr – 15:15 Uhr**

**Sicherheitszonen in der LAN-Infrastruktur**

- Seiteneffekte konvergenter Netze auf die Sicherheit
- Sicherheitsinfrastrukturen bei Gefährdungen von innen
- Firewalls und Protokolle in verteilten Systemen
- Authentifizierung und Autorisierung am LAN-Zugang:  
Techniken und ihre Grenzen
- Zugang für Gäste und Fremdfirmenmitarbeiter

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

**15:15 Uhr – 16:00 Uhr**

**Entwicklung eines Konzepts für Security Incident Handling**

- Einbettung des Security Incident Handlings in die vorhandenen Prozesse (Sicherheitsprozess, Business Continuity, Disaster Recovery)
- Komponenten des Security Incident Handlings und Berücksichtigung der verschiedenen Bedrohungsphasen
- Definition eines Security Incident Handling Prozesses
- Erfahrungen bei der Umsetzung

*Sven Schumann,  
HUK-Coburg-Allgemeine Versicherung AG*

**16:30 Uhr – 17:15 Uhr**

**Business Continuity Planning in der IT-Praxis**

- Einführung in die BCP-Thematik
- Einsatz eines Scoring-Verfahrens bei der Bestimmung kritischer Prozesse
- Notfallpläne und ihre Praxistauglichkeit
- Test, Pflege und Revision der Planung

*Holm Diening,  
GAI NetConsult GmbH*

**17:15 - 18:00 Uhr**

**Security Awareness - Mitarbeitersensibilisierung**

- Mitarbeiter als „letzte Bastion“ der IT-Sicherheit
- Das 4-Phasen-Konzept einer Awareness-Kampagne
- Zentrale Erfolgsfaktoren
- Praxisbeispiele

*Dirk Fox,  
Secorvo Security Consulting GmbH*

**11:45 - 12:15 Uhr Kaffeepause  
13:00 - 14:30 Uhr Mittagspause  
16:00 - 16:30 Uhr Kaffeepause  
ab 18:30 Uhr Happy Hour**

## Programmübersicht IT-Sicherheits-Forum 2006

**Mittwoch, 10.05.06 Praxis-Workshops - Die Durchführung der Workshops wird am Teilnehmerinteresse ausgerichtet****Workshops 09:00 - 12:30 Uhr****Workshop 1:****Einsatz von netzwerk-basierten IPS**

- IPS versus IDS und Abgrenzung zu Firewall: Motivation für IPS
- Funktionsweise von IPS: Techniken zur Erkennung von Angriffen
- Aufbaukonzepte, Redundanz und Performance
- Zu beachtende Aspekte bei der Auswahl von IPS
- Produktbeispiele
- Praktische Erfahrungen

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

**Workshop 2: Modern Hacking - Know your Enemy - Live-Demo von Angriffstechniken**

- Schwachstellentrends 2005 / 2006
- Passive Zielfindung per Suchmaschine (Google-Hacking und Co.)
- Moderne Exploittechniken und -frameworks
- Angriffe auf Applikationsebene
- Rootkits und Anti-Forensics

*Björn Fröbe, GAI NetConsult GmbH*

**Workshop 3: Business Continuity Planning im IT-Umfeld - Live-Demo eines Tools**

- Einführung: Erfordernisse, Fälle aus der Praxis, Begriffsdefinition
- Gesetzliche und andere Anforderungen an Unternehmen
- Vorgehen bei der Business Impact Analyse und der Risikoanalyse
- IT-relevante Bestandteile der Notfallorganisation und Arten von Notfallplänen
- Praktische Vorgehensweise in der Planungsphase
- Teststrategien, Training, Awareness und Pflege
- Anforderungen an BCP-Planungstools, wichtige Produkte am Markt
- kurze Demonstration der Planung und Pflege an einem ausgewählten Produkt

*Holm Diening, GAI NetConsult GmbH*

**Workshop 4: Sicherheit von BlackBerry und Alternativlösungen - Vergleich unterschiedlicher Lösungen**

- Einführung und Überblick zu den im Workshop vertretenen Produkten
- Sicherheitsaspekte einer Mobile PIM-Lösung:
  - Schutz der Endgeräte
  - Schutz der Kommunikation
  - Schutz der zentralen Server
  - Zentrales Management und Überwachung
- Live-Demonstrationen der verschiedenen Lösungen
- Auswahlkriterien für die eigene Produktauswahl

*Frank Breitschaft, GAI NetConsult GmbH*

**Workshops 14:00 - 17:00 Uhr****Workshop 5:****IT-Security Best Practice - Top-10 Tips and Tricks in der Diskussion****Vorgesehene Themen sind:**

- Konfiguration von Webbrowsern
- Sicherung von Webservern
- Sichere E-Mail
- Aufbau einer sicheren Adminumgebung
- VPN (IPsec und SSL)
- Secure RAS

*Björn Fröbe, Dr. Torsten Johr,  
GAI NetConsult GmbH,  
Dr. Simon Hoff, Andreas Meder,  
ComConsult Beratung und Planung GmbH,*

**Workshop 6:****Intelligente Analyse von Security Log Files**

- Security Log File Korrelation mit Aufzeichnung und Rekonstruktion kritischer Ereignisse
- Welche Art der Event-Korrelation macht Sinn?
- Anforderungen an einen Tool-Einsatz
- Vorgehensweise bei der Suche nach „Critical Events“
- Ergänzung forensischer Untersuchungen
- Nutzung der Erkenntnisse auch für Basel II, Sarbanes-Oxley etc.

- Praktische Beispiele und Hands-On  
*Paul Hoffmann, DATAKOM GmbH,  
Peter Weinlich, GTEN AG*

**Workshop 7: User Identity based access control- Zugriffsschutz auf allen Ebenen Live-Demos unterschiedlicher Technologien**

- Einführung: Authentisierung und Autorisierung - Wer bin ich und was darf ich
- Authentisierung und Autorisierung gestern, heute und morgen
- Zugriffssicherung - Protokolle und Methodik im Überblick NAP, NAC, 802.1X in der Praxis
- Identity based access control: Grenzen ziehen, wie und wo
- Betrachtung rechtlicher Aspekte

*Carsten Poppe,  
entrada Kommunikations GmbH*

**Workshop 3: Business Continuity Planning im IT-Umfeld - Live-Demo eines Tools**

- Einführung: Erfordernisse, Fälle aus der Praxis, Begriffsdefinition
- Gesetzliche und andere Anforderungen an Unternehmen
- Vorgehen bei der Business Impact Analyse und der Risikoanalyse
- IT-relevante Bestandteile der Notfallorganisation und Arten von Notfallplänen
- Praktische Vorgehensweise in der Planungsphase
- Teststrategien, Training, Awareness und Pflege
- Anforderungen an BCP-Planungstools, wichtige Produkte am Markt
- kurze Demonstration der Planung und Pflege an einem ausgewählten Produkt

*Holm Diening,  
GAI NetConsult GmbH*

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

**Donnerstag, 11.05.06****9:00 Uhr - 10:00 Uhr****Projektbericht: IT-Sicherheit nach BS 7799**

- Ziel: Beratung zu organisatorischen und strategischen IT-Sicherheitsmaßnahmen
- Anwendung von ISO-Standard 17799 und BS 7799-2
- Pflichtenheft, IT-Assessment, Risikoanalyse
- Erstellung von Security Policy, Notfallkonzept und Sicherheitshandbuch

*Frank Spanier,  
DKV Euro Service GmbH & Co KG,  
Stefan Schänzer,  
BDG GmbH & Co KG*

**10:00 Uhr - 11:00 Uhr****Prozessorientiertes IT-Sicherheitsmanagement mit ITIL**

- ITIL: die Vorstellung
- Der Prozess ITIL Security Management
- Maßnahmen und Implementierung
- Koexistenz mit ITSM-Standards

*Christian Aust,  
.consecco*

**11:30 Uhr - 12:30 Uhr****Projektbericht: Aufbau eines sicheren Extranet-Webportals**

- Projektstart: Business vs. Security Requirements
- Durchführung einer Risikoanalyse
- Aufbau einer Schutzlösung mit Web Application Firewall und Access Management
- Aufbau der zugehörigen Sicherheitsorganisation

*Martin Noll,  
Schering AG*

**13:45 Uhr - 14:45 Uhr****Evaluierung von Web Application Firewalls**

- Evaluierungskriterien des Web Application Security Consortiums
- Überblick zu den am Markt verfügbaren Produkten
- Bewertung und KO-Kriterien in einzelnen Szenarien
- Hinweise für die eigene Produktauswahl

*Frank Breitschaft,  
GAI NetConsult GmbH*

**14:45 Uhr - 15:45 Uhr****Sicherheit für service-orientierte Architekturen (SOA)**

- SOA - ein Überblick
- Technische Grundlagen: XML Web Services, Architekturprinzipien
- Umsetzung von SOA-Sicherheit
- Vorstellung eines Fallbeispiels

*Sebastian Staamann,  
PrismTech GmbH*

**15:45 Uhr****Zusammenfassung und Schlusswort**

*Detlef Weidenhammer,  
GAI NetConsult GmbH*

**11:00 - 11:30 Uhr Kaffeepause**  
**12:30 - 13:45 Uhr Mittagspause**  
**16:00 Uhr Ende der Veranstaltung**

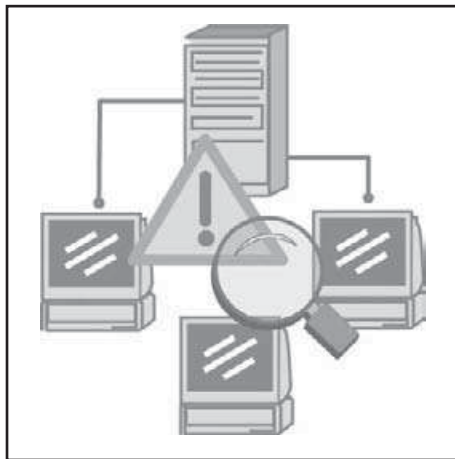
Frühjahrs-Kongress

# Gefahrenmeldetechnik und Objektüberwachung im Netz 2006

Die Comconsult Akademie veranstaltet vom 15. - 16. Mai das „Gefahrenmeldetechnik und Objektüberwachung im Netz 2006“ in Köln.

Der Ruf nach konvergenten Netzen macht vor dem Bereich der Gefahren- und Meldetechnik nicht halt, die Nachfrage nach einer Nutzungsmöglichkeit von IP-basierenden Netzen für Videoüberwachung, Einbruchmeldetechniken, Brandmelder, Zutrittskontrollen und ähnlichem nimmt rapide zu. Sowohl auf der Seite der klassischen Gebäudeüberwachungstechnik wie auch bei den IT-Spezialisten herrscht Unsicherheit darüber, welche dieser klassischen Techniken bereits heute durch IP abgedeckt werden können.

Das ComConsult-Forum „Gefahrenmeldetechnik und Objektüberwachung im Netz 2006“ führt die bereits 2005 im gleichnamigen Forum begonnene Analyse der Technologie-, Markt- und rechtlichen Situation fort, und gibt wesentliche Empfehlungen zur Einführung dieser neuen Techniken. Neben der Überarbeitung der Themen des Forums von 2005 werden vollkommen neue Themen Gegenstand der Veranstaltung sein.



Im Einzelnen geht das Forum auf folgende Fragen ein:

- Was leistet eine IP-basierende Infrastruktur im Bereich der Gebäudemeldetechnik heute?
- Welche Akzeptanz finden IP-basierende Lösungen bei den Versicherungen oder Sachverbänden?
- Welche Grundelemente sind vorzusehen, um Überwachungs- und Melde-

technik in IP-basierenden Netzen zu implementieren? Wie sehen die Erfahrungen bei erfolgreicher Einführung dieser neuen Techniken aus?

- Sind besondere QoS-Anforderungen an moderne Datennetze zu stellen, die eine Einführung erst möglich machen?
- Sind IP-basierende Netze wirklich so unsicher, dass sie nicht für „Security Anwendungen“ genutzt werden können?
- Wie ist ein Netz aufzubauen, um höchste Verfügbarkeit sicherzustellen?
- Welche Vorteile liefert eine Netzstrukturierung auf der Ebene 3?
- Wie lassen sich die aktuellen Entwicklungen im Bereich der WLAN-Techniken nutzen (Beispiel: IEEE 802.11n)?
- Warum steigt die Verfügbarkeit einer Videoüberwachung durch Nutzung von IP?
- Wo liegen die qualitativen Unterschiede der verschiedenen Überwachungstechniken?
- Welche Normen lassen netzwerkbasierende Gefahrenmeldetechniken zu?
- Müssen andere Komponenten eingesetzt werden oder lassen sich Standard-Bürokomponenten verwenden?

Fax-Antwort an ComConsult 02408/955-399

## Anmeldung Gefahrenmeldetechnik und Objektüberwachung im Netz 2006

Ich buche den Kongress  
**Gefahrenmeldetechnik und  
Objektüberwachung im Netz 2006**  
vom 15.05. - 16.05.06 in Köln  
zum Preis von nur € 1.590,- zzgl. MwSt.

**mit Report**  
„Ethernet in Industrie-Umgebungen“  
zum Preis von nur € 338,- zzgl. MwSt.

**ohne Report**

Bitte reservieren Sie für mich  
ein Hotelzimmer

vom \_\_\_\_\_ bis \_\_\_\_\_ 06

Vorname \_\_\_\_\_

Nachname \_\_\_\_\_

Firma \_\_\_\_\_

Abteilung \_\_\_\_\_

Telefon \_\_\_\_\_

Fax \_\_\_\_\_

Straße \_\_\_\_\_

PLZ, Ort \_\_\_\_\_

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

eMail \_\_\_\_\_

Unterschrift \_\_\_\_\_

## Programmübersicht Gefahrenmeldetechnik und Objektüberwachung im Netz 2006

### Montag, den 15.05.2006

#### 10:00 bis 11:15 Uhr

##### Integration von Gefahrenmanagement in IP-Netzen: Probleme und Lösungen

- Schwachstellen von IP-Netzen hinsichtlich Verfügbarkeit, Sicherheit, Echtzeitfähigkeit
- Welche Netzstrukturen bieten die höchste Verfügbarkeit?
- Erhöhung der Sicherheit von IP-Netzen
- Verfahren für die Trennung verschiedener Anwendungen in der selben Netzinfrastruktur
- Wie können in IP-Netzen garantierte Übertragungszeiten sichergestellt werden?

*Dr.-Ing. Behrooz Moayeri,*

*ComConsult Beratung und Planung GmbH*

#### 11:45 bis 12:30 Uhr

##### Integrationsmöglichkeit von Fremdgewerken

- Wichtige Basisfunktionen
- Einsatzschwerpunkte: Was muss, sollte und kann integriert werden (EMA, GLT, BMA, Video usw.)
- Schnittstellenproblematik (herstellerspezifische, OPC, Bacnet, SNMP, Patientenruf)
- Alarmbehandlung
- Sondersysteme (reine Alarmserver) Produkte wie DAKS und NewVoice
- Entscheidungshilfen und Herstellerübersicht

*Dipl.-Ing. Holger Häntzschel,*

*SSMB Service-, Sales und Managementberatungs GmbH*

#### 12:30 bis 13:15 Uhr

##### Netzbasierende Gefahrenmeldetechnik (Brand/Einbruch)

- Lassen aktuelle Normen Netzwerklösungen zu?
- Kocht jeder sein eigenes Süppchen?
- Wie kommen Gefahrenmeldungen ins LAN?
- Welche Funktionen einer Gefahrenmeldeanlage sind netzwerkfähig?
- Entwicklung und Trends

*Peter Loibl,*

*VON ZUR MÜHLEN'SCHE GmbH*

#### 14:45 bis 15:30 Uhr

##### Integrale Gefahrenmanagementsysteme? Alles ist möglich, was ist sinnvoll ?

- Realisierungskonzept eines Gefahrenmanagementsystems
- Wirtschaftlichkeitsbetrachtung
- Intuitive Bedienerinterfaces und effektive Systempflege
- Ereignisgesteuertes Notfallmanagement und Protokollierung
- Herstellerneutrale Integration von bestehenden Anlagen
- Praxisbeispiele aus verwirklichten Objekten
- Live Systemdemonstration einer typischen Anwendung

*Lothar Marth,*

*Novar GmbH by Honeywell*

#### 15:30 bis 16:30 Uhr

##### Quality of Service im Dienste von Gefahrenmanagement

- Warum ist Quality of Service im Zusammenhang mit Gefahrenmanagement wichtig?
- Gesamtarchitektur für Quality of Service
- Quality of Service in drahtgebundenen LAN
- Quality of Service in Wireless LAN
- Quality of Service in WAN

*Dr.-Ing. Behrooz Moayeri,*

*ComConsult Beratung und Planung GmbH*

#### 17:00 bis 17:45 Uhr

##### Videoüberwachung über IP (Anforderungen, Lösungen, Grenzen)

- Motivation
- Anforderungen an die Video-Qualität
- Welche Funktionen können implementiert werden?
- Anforderungen an das Netz
- Aufbau von „Video-Netzwerken“

*Dipl.-Ing. Hartmut Kell,*

*ComConsult Beratung und Planung GmbH*

**11:15 - 11:45 Uhr Kaffeepause**  
**13:15 - 14:45 Uhr Mittagspause**  
**16:30 - 17:00 Uhr Kaffeepause**  
**ab 18:00 Uhr Happy Hour**

### Dienstag, den 16.05.2006

#### 9:00 bis 10:00 Uhr

##### Sicherheitsanforderungen von Gefahrenmeldelösungen

##### in Lokalen Netzwerken und ihre Umsetzung

- Bedrohungen im LAN und Auswirkungen auf Gefahrenmeldesysteme
- Sicherheitsmaßnahmen für die Übertragung der Überwachungs- und Meldedaten
- Verschlüsselung und Authentifizierung: Was muss sein und was ist überhaupt sinnvoll möglich?
- Schutz der Komponenten und der Übertragungswege eines Gefahrenmeldesystems

*Dr. Simon Hoff,*

*ComConsult Beratung und Planung GmbH*

#### 10:00 bis 10:30 Uhr

##### Praktische Umsetzung von Videoüberwachung über IP (Projektbeispiel)

- Was war die Motivation für Video über IP?
- Welche Anforderungen an die Video-Qualität wurden gestellt?
- Welche Funktionen wurden implementiert?
- Welche Anforderungen haben wurden an das IP-Netz gestellt
- Wie wurde das „Video-Netzwerk“ aufgebaut?
- Anforderungen an die Video-Qualität

*Jürgen Clemens, Harry Kaulen,*

*TFA Gesellschaft für Kommunikationselektronik GmbH*

#### 11:00 bis 11:30 Uhr

##### IPC und Gefahrenmeldung - Synergieeffekte und neue Anwendungen

*Bert-Henrik Czaya,*

*CISCO Systems GmbH*

#### 11:30 bis 12:15 Uhr

##### Intercom over IP

- IoIP® - Intercom over IP - Möglichkeiten, Unterschiede, Lösungen
- Was ist Intercom over IP?
- Unterschiede zu Telekommunikationstechniken (IoIP/VoIP)
- Lösungsbeispiele

*Harald Weber,*

*SCHNEIDER INTERCOM GmbH*

#### 13:30 bis 14:45 Uhr

##### Funküberwachung: Stabilität, Verfügbarkeit, Sabotierbarkeit

- Was leisten die Datendienste der Mobilfunknetze (GSM/GPRS, UMTS) und welche Einsatzbereiche sind sinnvoll
- Bluetooth und WLAN in der Funküberwachung
- Sicherheit in Funknetzen
- Stand der Dinge bei ZigBee

*Dr. Simon Hoff,*

*ComConsult Beratung und Planung GmbH*

#### 14:45 bis 15:30 Uhr

##### Sicherheitsrelevante Meldungen über IP

- Anforderungen
- Berücksichtigung von vorhandenen Strukturen
- Nutzung kundeneigener Datennetze für sicherheitsrelevante Meldungen über IP (Projektbeispiele)

*Knut Schneidmesser,*

*Bosch Sicherheitssysteme GmbH*

#### 15:30 bis 16:15 Uhr

##### Nutzeranforderungen zu Gefahrenmeldesystemen im RZ

- Raumüberwachung (Einbruchmeldeanlage, Türüberwachung, Kameras, Brand/Rauch, Temperatur, rel. Luftfeuchte, Wasser)
- Infrastrukturüberwachung (Klimaanlage, Stromversorgung, USV, Notstrom)
- Professionelle Lösungen für große RZ
- Kleine Lösungen für kleine RZ und wichtige Technikräume

*Mark Groten,*

*ComConsult Beratung und Planung GmbH*

**10:30 - 11:00 Uhr Kaffeepause**  
**12:15 - 13:30 Uhr Mittagspause**  
**ca. 16:15 Ende der Veranstaltung**

## Zweitthema

# Business Continuity Planning

Fortsetzung von Seite 1



Holm Diening ist seit seinem Studium der Elektrotechnik als IT-Sicherheitsberater - zunächst selbständig, mittlerweile für die GAI NetConsult GmbH - tätig. Seine Schwerpunkte liegen im IT-Sicherheitsmanagement (ISO 27001), der Notfallplanung (Business Continuity Planning) und der Erstellung von organisatorischen und technischen Sicherheitsrichtlinien. Herr Diening hat umfangreiche Erfahrungen als Referent bei Sicherheitsschulungen und Security Awareness Trainings. Er besitzt die Zertifizierung als „Certified Information Systems Security Professional (CISSP)“ durch das (ISC)<sup>2</sup>.

„Wenn das passiert, dann können wir hier sowieso einpacken!“ Diese oder eine ähnliche Antwort erhält man nicht selten, wenn in Unternehmen nach der Vorbereitung auf einen eventuellen Großschaden gefragt wird. Dabei klingt immer ein wenig die Einstellung mit, dass man sich auf wirkliche Katastrophen ohnehin nicht ausreichend vorbereiten könne und dass sich so etwas für diese extrem seltenen Fälle auch gar nicht lohne. Die Verantwortung gegenüber den eigenen Mitarbeitern, den Aktionären, aber auch den Kunden, verbietet jedoch hier zu pokern. Je länger ein Unternehmen besteht und je größer es ist, desto eher wird es sich einmal einer solchen Situation stellen müssen. Ohne ein durchdachtes und erprobtes Notfallkonzept ist ein koordiniertes und zielführendes Handeln der Beteiligten im Ernstfall jedoch nicht möglich. Eine angemessene Vorbereitung auf Notfallszenarien wird daher auch als Bestandteil ordnungsgemäßer Corporate Governance angesehen. In Deutschland existiert bisher keine eigene gesetzliche Vorschrift zur Notfallvorsorge. Es werden jedoch einige Gesetze in dieser Richtung interpretiert. Beispiele hierfür sind:

- § 91 Abs. 2 AktG (Früherkennung von Risiken)
- § 43 Abs. 1 GmbHG (Sorgfaltspflichten)

Konkrete Forderungen an eine Notfallvorsorge ergeben sich aber aus einigen branchenspezifischen Bestimmungen und Verordnungen. Als jüngstes Beispiel seien hier die Mindestanforderungen an das Risikomanagement (MaRisk) des Bundesamtes für Finanzdienstleistungsaufsicht genannt. Hier wird in Abschnitt 7.3 explizit ein Notfallkonzept gefordert.<sup>1</sup>

Weitere wichtige Impulse für Rechtsgrundlagen könnten sich auch aus dem

KRITIS Projekt<sup>2</sup> des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ergeben. Im Rahmen des „Nationalen Plans zum Schutz kritischer Infrastrukturen“ des Bundesinnenministeriums will das BSI entsprechende Vorgaben für den IT-Bereich entwickeln. Eine konkrete Umsetzung in gesetzliche Anforderungen steht aber noch aus.

## Begriffe und Abkürzungen

Nicht ganz einfach ist im Themenkomplex der Notfallplanung die Zuordnung einiger Fachbegriffe. Bei der Auseinandersetzung mit der Materie wird man feststellen, dass hier oft noch nicht einmal Einigkeit bei Bezeichnung der eigenen Fachdisziplin herrscht.

Dies betrifft zunächst die Begriffe „Business Continuity Management“ und „Business Continuity Planning“. Meist werden diese beiden Bezeichnungen in der amerikanischen (Planning) und der britischen Literatur (Management) synonym verwandt. In beiden Fällen sind hierbei alle Maßnahmen zur Beibehaltung der Arbeitsfähigkeit einer Organisation während und nach einer unvorhergesehenen Betriebsunterbrechung gemeint. Der britische defacto-Standard PAS 56 (mehr zu Standards im nächsten Abschnitt) kennt hingegen durchaus Unterscheidungspotential. Dieses speist sich vor allem aus seiner übergeordneten Betrachtungsweise. Business Continuity Management ist hier ein ganzheitlicher Managementprozess, der a) mögliche Bedrohungen für eine Organisation durch unvorhergesehene Ereignisse identifiziert und b) ein Framework zur Verbesserung der Widerstands- und Reaktionsfähigkeit eines Unternehmens bei solchen Ereignissen zum Schutz der Interessen der Anteilseigner, des Images des Unternehmens und der

Wertschöpfungskette bildet. Nach dieser Definition geht der Begriff BCM also weit über die Erhaltung der Geschäftsprozesse bei Katastrophen oder ähnlichen Vorfällen hinaus.

Ebenfalls nicht eindeutig ist die Benutzung der Abkürzung „BCP“, die für „Business Continuity Planning“ und auch für den „Business Continuity Plan“, also das Ergebnis des „Planning“, verwendet wird.

Der Autor dieses Artikels folgt bei der Unterscheidung zwischen Business Continuity Management und Planning der Darstellung des PAS 56. Da wir uns hier vor allem mit der Planung von Abläufen in konkreten Notfällen beschäftigen wollen, fassen wir alle Maßnahmen mit dieser Zielsetzung unter dem Begriff „Business Continuity Planning“ zusammen.

## Business Continuity Planning im IT-Bereich

Die Aufrechterhaltung oder der schnelle Wiederanlauf des Geschäftsbetriebes nach einem Notfall erfordert das koordinierte Handeln in den unterschiedlichsten Ebenen. Der IT-Bereich ist hierin nur eine Facette, deren Bedeutung von der Branche des jeweiligen Unternehmens abhängt. Nicht-IT Aspekte eines BCP wären der präventive Schutz kritischer Infrastrukturen, die Bereitstellung von Produktions- und Büroflächen, die Kommunikation mit den Medien und auch die manuelle Überbrückung wichtiger Geschäftsprozesse im „Offline-Modus“, also ohne die zentrale IT.

Folgende Bestandteile einer Notfall- oder Katastrophenvorsorge sind hingegen für den IT-Bereich relevant (rechts in Abbildung 1):

<sup>1</sup>[http://www.bafin.de/rundschreiben/89\\_2005/051220.htm](http://www.bafin.de/rundschreiben/89_2005/051220.htm)

<sup>2</sup><http://www.bsi.bund.de/fachthem/kritis/>

## Business Continuity Planning

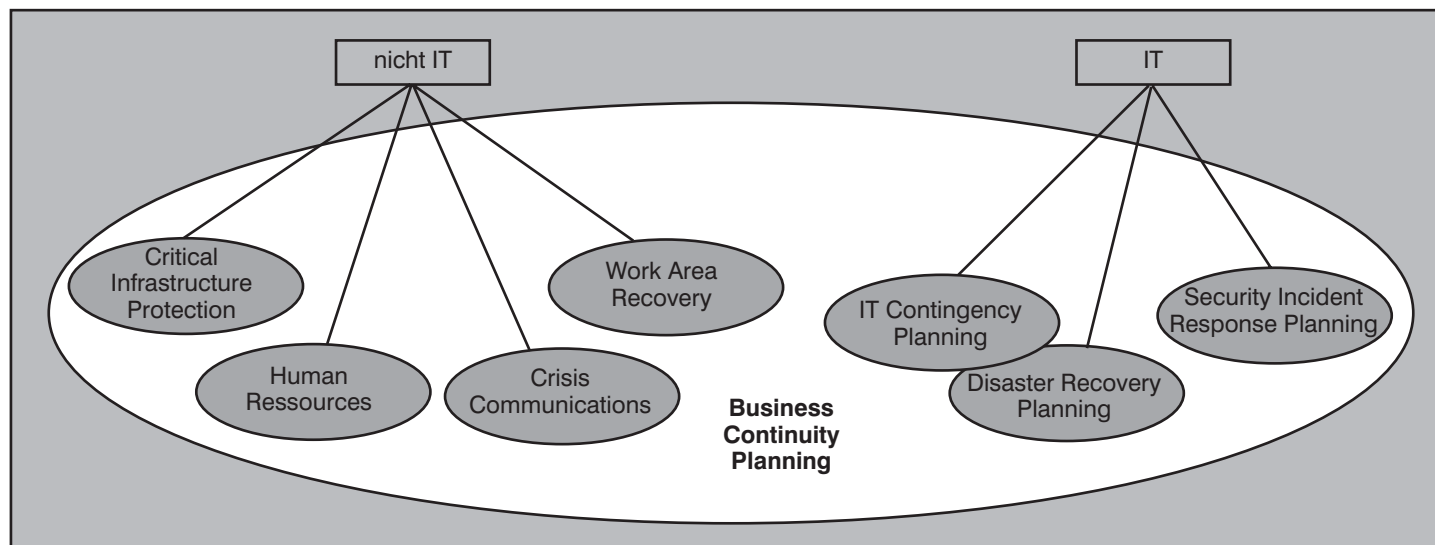


Abbildung 1: Bestandteile des Business Continuity Planning

**IT-Contingency Plan (IT-Notfallplan)**

Ein IT-Notfallplan wird für die Aufrechterhaltung der Betriebsbereitschaft wesentlicher Applikationen erstellt. Daher existieren in Unternehmen mehrere Notfallpläne für die unterschiedlichen Anwendungen. Oft werden solche Pläne bereits durch externe Systembetreuer oder die Anwendungs- und Systemhersteller mitgeliefert und gewartet. So kann eine IT-Abteilung getrennte Notfallpläne für die Finanzapplikationen, das ERP-System oder den Mailserver haben.

**IT-Disaster Recovery Plan**

Wie der Name bereits vermuten lässt, handelt es sich hier um die Vorbereitung auf Katastrophen und ähnliche Ereignisse, die einen IT-Betrieb in den bisherigen Räumlichkeiten mittelfristig unmöglich machen. Meistens handelt es sich daher um Pläne, die eine Wiederaufnahme des IT-Betriebes an einem Ausweichstandort zum Gegenstand haben. Es kann hierbei an einigen Stellen zu Überschneidungen mit den IT-Notfallplänen kommen (siehe Abbildung 1), obwohl diese im Allgemeinen keine schwerwiegenden Ereignisse behandeln, die auch eine Verlagerung von IT erforderlich machen.

**Cyber Incident Response Plan (CIRP)**

Auch der Ausbruch von Computer Viren in einem Netzwerk oder der vorsätzliche Angriff eines Crackers können die Verfügbarkeit von IT-Anwendungen stören. Ein CIRP dient zur frühzeitigen Erkennung solcher Vorfälle, der schnellen und angemessenen Reaktion und der Schadensbegrenzung.

**Wichtige Standards und Best Practices**

Die Thematik der Notfallplanung findet sich im Fokus diverser Standards und Best Practices. Je nach Herkunft sind diese eher IT-orientiert oder beschreiben Notfallplanung aus der Sicht der Geschäftsprozesse.

Der British Standard 7799-1 oder die gleich lautende ISO 17799 beschreiben auf 10 Seiten die Einbindung der Information Security in das BCM. Dabei wird die Existenz eines übergeordneten Business Continuity Management Prozesses im Unternehmen bereits vorausgesetzt. Das IT-Grundschutzhandbuch des Bun-

desamtes für Sicherheit in der Informationstechnik enthält hierfür einen eigenen Baustein: „Notfallvorsorge-Konzept“. Dieser beschreibt schrittweise den Aufbau und die Pflege eines Notfallkonzeptes aus Sicht der IT. Das Subset „Service Delivery“ der IT Infrastructure Library (ITIL) befasst sich im Abschnitt „IT Service Continuity Management“ über knapp 50 Seiten mit dem gesamten Prozess der IT-Notfallplanung, den Teststrategien, der Sensibilisierung und den Verantwortlichkeiten. Ähnlich strukturiert, aber noch ausführlicher, ist die amerikanische NIST Special Publication 800-34 „Contingency Planning Guide for Information Technology Systems“.

**Backlog Processing**

Aufarbeitung des Arbeitsrückstandes

**BCM (Business Continuity Management)**

Ganzheitlicher Ansatz zur Aufrechterhaltung des Geschäftsbetriebes bei unvorhergesehenen Ereignissen

**Business Continuity Planning**

Planung von Maßnahmen zur Aufrechterhaltung oder Wiederherstellung des Betriebes in Notfällen. Hinweis: Die Abkürzung BCP bedeutet auch den „Business Continuity Plan“, also das Produkt des Business Continuity Plannings

**BIA (Business Impact Analyses)**

Analyse der Auswirkungen von unvorhergesehenen Ereignissen auf wichtige Geschäftsprozesse

**IT-CP (Contingency Plan)**

Plan zur Aufrechterhaltung wichtiger IT-Dienste bei größeren Störfällen

**IT-DRP (Disaster Recovery Plan)**

Plan zur Wiederherstellung des IT-Betriebes nach einer Katastrophe

**MCA (Mission Critical Activity)**

Ein Kernprozess, der für den Geschäftsbetrieb unabdingbar ist

**RTO Recovery Time Objective**

Zeitraum, innerhalb dessen ein Prozess wieder hergestellt sein muss

**RPO Recovery Point Objective**

Zeitpunkt (z.B. Quartalsabschluss), zu dem ein Prozess wieder hergestellt sein muss

Abbildung 2: Begriffe und Abkürzungen (alphabetisch)

Business Continuity Planning

Alle diese Standards haben ausschließlich die IT-Notfallplanung und deren Beitrag zur Aufrechterhaltung der Geschäftsprozesse zum Gegenstand. Weiter gefasst und ohne speziellen Fokus auf die IT ist die Publicly Available Specification (PAS) 56 „Guide to Business Continuity Management“, herausgegeben vom BCI (The Business Continuity Institute). Bemerkenswert ist dieser Standard vor allem deshalb, weil sich seine internationale Etablierung abzeichnet. In einer aktuellen Pressemitteilung des BSI (hier: British Standards Institute)<sup>3</sup> wird die PAS 56 gegen Ende 2006 ein offizieller British Standard.<sup>4</sup> Die Spezifikation soll dabei als BS 25999 Serie aufgenommen werden und zwar sowohl als BS 25999-1:2006 „Code of practice for business continuity management“ gegen Ende diesen Jahres

und später, im Frühjahr 2007, auch als BS 25999-2:2006 „Specification for business continuity management“. Damit ist für die künftigen BCM Standards des BSI die gleiche Trennung zwischen „Code of practice“ und „Specification“ vorgesehen, wie beim BS 7799. Zusammen mit der ebenfalls angestrebten Adaption der Standards durch die ISO entstehen hier wohl, zumindest im europäischen Raum, die wichtigsten Standards im Bereich des Business Continuity Managements.

**Phasen des Business Continuity Planning**

Dieser Abschnitt beschreibt die einzelnen Phasen des Business Continuity Planning, wobei die IT-relevanten Bestandteile im Vordergrund stehen sollen. Die nachste-

hende Abbildung 3 gibt einen Überblick über ein aus fünf getrennten Abschnitten bestehendes Modell. Es ist angelehnt an das Vorgehensmodell für IT Service Continuity Management aus dem ITIL Service Delivery Handbuch.

**Phase 1: Initialisierung**

Die erste Phase ist, langfristig gesehen, zugleich die wichtigste. Hier gilt es, die genauen Ziele zu definieren, sowie den Umfang und die Vorgehensweise zu bestimmen. Gleichzeitig muss bereits hier das Management von der Notwendigkeit des Projektes und auch der Weiterführung als nachfolgender Prozess überzeugt werden. Gerade für den Prozess werden finanzielle und personelle Ressourcen benötigt, die in der ersten Phase der Planung thematisiert werden müssen.

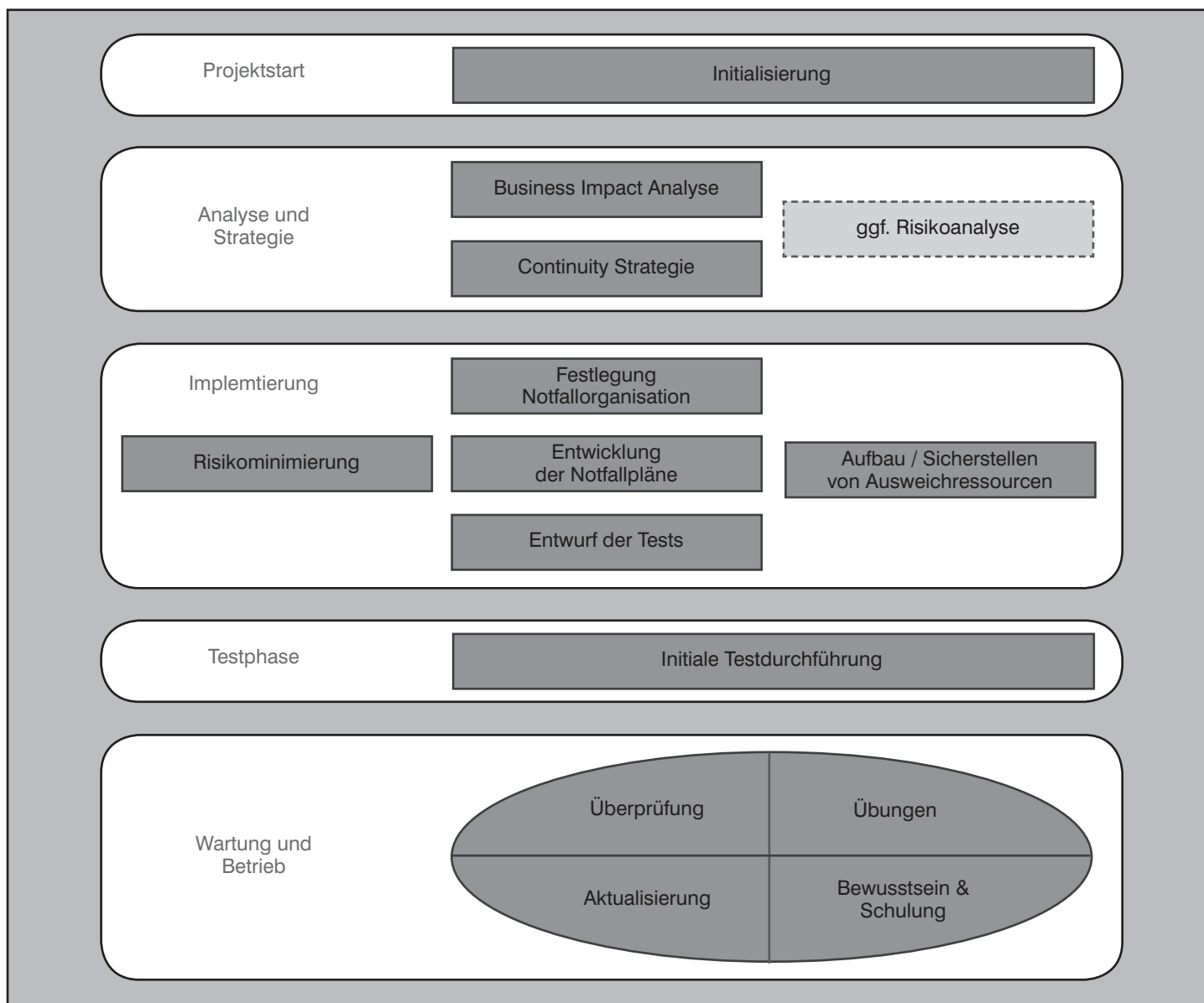


Abbildung 3: Phasenmodell in Anlehnung an ITIL IT Service Continuity Management

<sup>3</sup><http://www.thebci.org>

<sup>4</sup>[http://www.bsi-global.com/Business\\_Information/PressReleases/pas56.xalter](http://www.bsi-global.com/Business_Information/PressReleases/pas56.xalter)

## Business Continuity Planning

Folgende Punkte sind wichtige Ergebnisse der ersten Phase:

- Zu erwartende Kosten, benötigte Ressourcen, geplante Dauer sind bekannt.
- Die Projektorganisation (Teamzusammensetzung, Rollen, Befugnisse, Reporting) ist abgestimmt.
- Ein Projektplan mit Meilensteinen existiert.
- Die BC-Policy mit Zielen und Scope wurde vom Management unterschrieben.
- Die Weiterführung des Prozesses nach Ende des Projektes ist sichergestellt.

### Phase 2: Analyse und Strategie

In der zweiten Phase schafft man die Grundlagen für die eigentliche Planung. In einer Business Impact Analyse werden zunächst wichtige Geschäftsprozesse identifiziert und die Auswirkungen möglicher Unterbrechungen analysiert. Die Auswirkungen sind dabei nicht nur monetärer Art und müssen in verschiedener Hinsicht bewertet werden. Wichtig ist dabei auch die Darstellung der Auswirkungen in Abhängigkeit der Dauer der Unterbrechung. Die Bewertung einer MCA (Mission Critical Activity) kann anhand eines Scoringverfahrens vorgenommen werden, das die Auswirkungen einer Unterbrechung durch ein Kennzahlen (zum Beispiel Schulnotensystem) beschreibt und anschließend die einzelnen Bewertungskriterien mit einem vorher festgelegten Schema gewichtet. Die Vergabe von Kennzahlen sollte dabei auf der Basis eines festgelegten Beurteilungsschlüssels erfolgen. So können finanzielle Auswirkungen in ihrer Höhe mit dem zu erwartenden Jahresgewinn verglichen werden. Auswirkungen auf die Reputation bewertet man zum Beispiel von „1“ für „keine Auswirkungen“ bis zu „6“ für „schwerwiegender langfristiger Imageschaden“. Ein solches Bewertungsschema könnte etwa folgendes Aussehen haben: (siehe Tabelle 1)

Anhand dieser Auswertung und anderer Kenntnisse über den jeweiligen Geschäftsprozess ergeben sich dann auch die RTO und RPO (siehe Abbildung 2). Die Mindestanforderungen an einen eingeschränkten Betrieb zur kurzfristigen Überbrückung von Notfällen (zum Beispiel mit weniger Personal oder unter Verzicht auf bestimmte Applikationen) müssen ebenfalls bekannt sein.

Nachdem die wichtigsten Geschäftsprozess und deren Kritikalität bestimmt sind, können nun jeweils mögliche Bedrohungen identifiziert und bewertet werden, die möglicherweise zu einer Unterbrechung führen. Gegebenenfalls, wenn der Prozess als besonders kritisch für das Unternehmen eingeschätzt wird, sollte man eine klassische Risikoanalyse hierfür bemühen.

Das Ergebnis für den IT-Bereich aus diesem Schritt ist eine priorisierte Liste von wichtigen Geschäftsprozessen, die von der IT abhängig sind und daher nach einer Unterbrechung im Bereich der IT nicht mehr oder nur eingeschränkt ablaufen können.

In Abhängigkeit der Ergebnisse der BIA und der organisatorisch/technischen Möglichkeiten erfolgt nun die Festlegung der Strategie zur Aufrechterhaltung der jeweiligen Geschäftsprozesse. Sämtliche Optionen im IT-Bereich lassen sich in drei Kategorien unterteilen:

- Risikominimierung
- Notfallplanung zur Wiederherstellung
- Ausweichlösungen

Die Maßnahmen im Bereich der Risikominimierung zielen darauf ab, einen Ausfall von kritischen IT-Anwendungen von vorn herein zu vermeiden. Dazu zählen zum Beispiel die Vermeidung von Single Points of Failure in der eingesetzten Hardware, der physikalische Schutz der IT-Infrastruktur oder die Nutzung von zwei verschiedenen Internet Providern.

Notfallpläne sollen im Bedarfsfall (wie: Serverausfall, Netzwerkunterbrechungen, Softwarefehler nach Versionswechsel) eine rasche Wiederherstellung der wichtigsten Applikationen an Ort und Stelle erleichtern.

Die Nutzung von Ausweichlösungen ist die Option für die Bewältigung der schwerwiegendsten Störfälle. Hier ist eine Verlagerung des IT-Bereiches an einen anderen Standort erforderlich. Inwieweit dieser neue Standort schon auf die Übernahme des RZ-Betriebes vorbereitet ist, hängt von der zulässigen Wiederherstellungsfrist (RTO) ab. Ausweichrechenzentren können ausgeführt sein als:

**Hot-Site**

- Betriebsbereites RZ mit vollständig duplizierter Hardware und aktueller Software, Daten können sofort eingespielt werden oder sind bereits vorhanden (Mirrored Site)

**Warm-Site**

- Zentrale IT steht bereit. Es fehlen noch Peripherie, Software und Daten.

**Cold-Site**

- Ein leeres RZ ohne jede Hardware. Stromversorgung, Klimatisierung und andere Infrastruktur sind jedoch vorhanden.

**MVRZ**

- Mobiles Vorsorge-Rechenzentrum. Es ist meist ähnlich ausgestattet wie eine Warm-Site, kann aber direkt vor Ort gebracht werden. Je nach dem, wie schwer bspw. das Firmengebäude betroffen ist, kann die RZ-Umgebung an Ort und Stelle oder auch an einer Ausweichlokation aufgebaut werden.

MCA:	1 Tag			2 Tage			1 Woche			2 Wochen			1 Monat		
	Note	Gew.	Bew.	Note	Gew.	Bew.	Note	Gew.	Bew.	Note	Gew.	Bew.	Note	Gew.	Bew.
Finanzielle Auswirkung															
Verlust von Reputation															
Rechtliche Konsequenzen															
Sicherheit von Personen															
Verlust von Konkurrenzvorteilen															
Auswirkungen auf den Marktanteil															
Aufwand für das Backlog Processing															
<b>Summe</b>															

Tabelle 1: Scorecard für die Bewertung der Auswirkungen einer Unterbrechung einer MCA

## Business Continuity Planning

Die Ergebnisse dieser Phase sind die Richtschnur für die eigentliche IT-Notfallplanung. Sie geben Auskunft über die Prioritäten bei der Wiederherstellung der einzelnen Business Applikationen und die Fristen, nach denen diese wieder bereit stehen müssen.

**Phase 3: Implementierung**

Die Implementierung eines Notfallkonzeptes erfolgt in drei Stufen: Der Festlegung einer geeigneten Notfallorganisation, der Erarbeitung von Alarmierungsketten und Ablaufplänen und sowie der Planung und Durchführung von Tests.

Die Notfallorganisation einer IT Abteilung sollte sich von der Organisationsstruktur im Tagesgeschäft kaum unterscheiden. Schließlich werden die Notfallpläne auch von den Fachbereichen entwickelt und betreut, die sie auch im Ernstfall ausführen sollen. Es müssen jedoch einige Punkte beim Aufbau der Notfallteams beachtet werden, die im Tagesgeschäft weniger relevant sind:

- Leitende Funktionen in Notfallteams sollten durch zwei Stellvertreter abgesichert sein.
- Die Anfahrtswege der Mitarbeiter von zu Hause sollten in der Teambildung berücksichtigt werden.
- Einige Mitarbeiter sind als Ersthelfer ausgebildet und haben im Notfall andere Verpflichtung. Sie stehen für die Notfallteams ggf. nicht zur Verfügung.
- Je nach Eskalation (Störung, Notfall, Krise) wird der Fachbereichs- oder Abteilungsleiter in einem übergeordneten Krisenstab des Unternehmens mitarbeiten und ist daher für interne Aufgaben nicht abkömmlich.
- Die Führungsqualitäten in Krisensituationen sollten bei der Teambildung mit berücksichtigt werden.

Ein weiterer organisatorischer Aspekt sind die Rahmenbedingungen für die zeitlich befristete Erweiterung von Befugnissen. Dies betrifft zum Beispiel die kurzfristige Beschaffung von Ersatzhardware durch die IT ohne den Umweg über den Einkauf, oder auch die Anordnung von Sonderschichten, Wochenendarbeit und Urlaubssperren ohne die Zustimmung des Personalbereiches.

Aus der Festlegung der Notfallorganisation erschließt sich im Wesentlichen auch die Definition von Alarmketten. Je nach Art des Vorfalls wird eine andere Stelle die Alarmkette auslösen, die jedoch am Ende immer die Alarmierung aller für den jeweiligen Notfall relevanten Teams zur Folge hat. (siehe Abbildung 5)

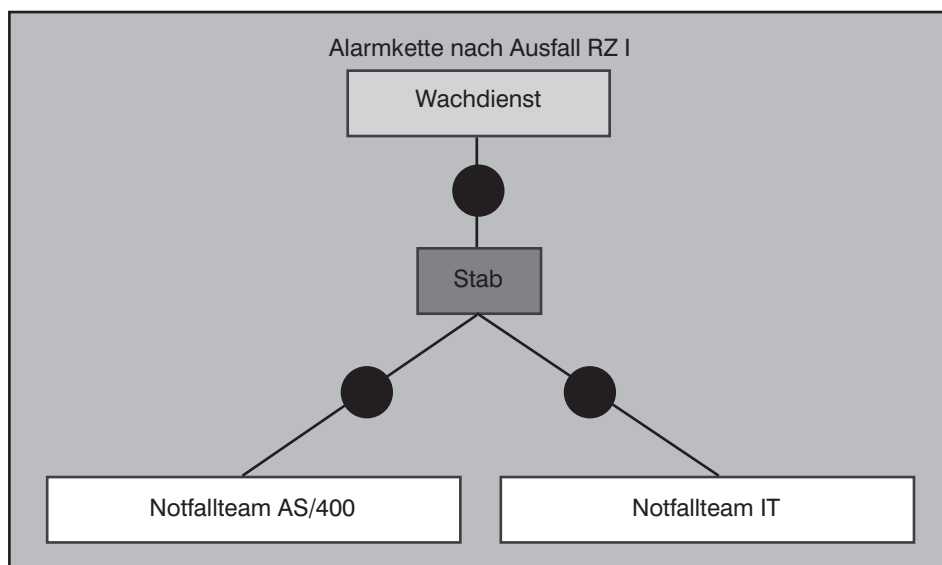


Abbildung 4: grafische Darstellung einer einfachen Alarmkette

Die Planung der eigentlichen Handlungsabläufe in einem Notfall enthält zunächst Pläne für übergeordnete Aspekte wie:

- Sofortmaßnahmen bei Unglücksfällen
- Bestandsaufnahme
- Umgang mit Medien
- Rettung von Backupbändern, Festplatten und anderen Datenträgern

Die nächste Ebene der Notfallpläne orientiert sich dann an den Aufgaben zur Erreichung eines eingeschränkten Betriebes zur einstweiligen Überbrückung der Not-situation (nach Festlegung aus Phase 2) und anschließend zur Wiederherstellung der vollständigen Betriebsbereitschaft.

Hierfür ist zunächst ein genauer Überblick über die IT-Infrastruktur und deren Beitrag zu den abzusichernden Geschäftsprozessen

## IT-Sicherheits-Forum 2006



**08.05. - 11.05.06  
in Bad Neuenahr**

Das IT-Sicherheits-Forum 2006 wird auch in diesem Jahr wieder die gerade aktuellen Themen zu Bedrohungsszenarien der IT-Sicherheit und zu den wichtigsten Schutzmaßnahmen aufgreifen. Dabei wird ein äußerst großer Wert auf Praxisnähe gelegt, dies zeigt sich insbesondere bei den technisch orientierten Workshops und den Praxisvorträgen, die direkt anwendbare „Tipps & Tricks“ für den Tagesbetrieb weitergeben.

Das Forum hat sich deshalb in den letzten Jahren zu einem stark besuchten Treffpunkt für alle Sicherheitsinteressierten entwickelt. An insgesamt vier Tagen werden angeboten:

- Erfahrungen aus aktuellen Sicherheitsvorfällen und Aufzeigen absehbarer Trends
- Neue Entwicklungen bei Sicherheitstechnologie und Sicherheitsorganisation
- Moderierte Workshops mit Produktvergleichen und Live-Demos
- Vertiefende Seminare und Tutorien

Moderation: Dipl.-Inform. Detlef Weidenhammer

Preis: € 2.190,- zzgl. MwSt. (4 Tage) bzw. € 1.790,- zzgl. MwSt. (3 Tage)



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

Business Continuity Planning

sen notwendig. Das klassische Vorgehen nach der Top-Down Methode beginnt dabei mit der Ermittlung der kritischen Geschäftsprozesse, bestimmt dann die dafür benötigten Applikationen und schließlich die zugrunde liegenden IT-Systeme. Ergänzend hierzu empfiehlt es sich im IT-Bereich einen eigenständigen Bottom-Up Ansatz zu verfolgen. Dieser beginnt mit der Strukturierung der Anwendungssysteme und des Datenbestandes und nimmt anschließend die Zuordnung zu den Geschäftsprozessen vor. Dies hat den Vorteil, dass die betreffenden BCP-Projektmitarbeiter zunächst ihr eigenes Metier von der

Basis her untersuchen können und dadurch wichtige Bindeglieder wie zum Beispiel Systeme zur Anpassung von Datenformaten oder Schnittstellenrechner nicht übersehen. Das Vorgehen hierfür lässt sich folgendermaßen zusammenfassen:

- Systematische Erfassung aller Anwendungssysteme und dort verarbeiteter Datenbestände
- Strukturierung und Zuordnung zu wichtigen Geschäftsabläufen
- Bestimmung gegenseitiger Abhängigkeiten von Anwendungen / Daten / IT-Systemen und Geschäftsabläufen

- Bestimmung funktionaler Abhängigkeiten (welche Daten und welche Systeme werden für welche Anwendung benötigt)
- Bestimmung zeitlicher Abhängigkeiten (in welcher Reihenfolge müssen welche Daten und Anwendungen zur Verfügung stehen)

Bei der anschließenden Erstellung der Notfallpläne für die ermittelte Systeminfrastruktur ist auf ein möglichst hohes Abstraktionsniveau zu achten. Einem Plan zur Wiederherstellung eines Datenbankservers sollte es egal sein, warum diese Wieder-

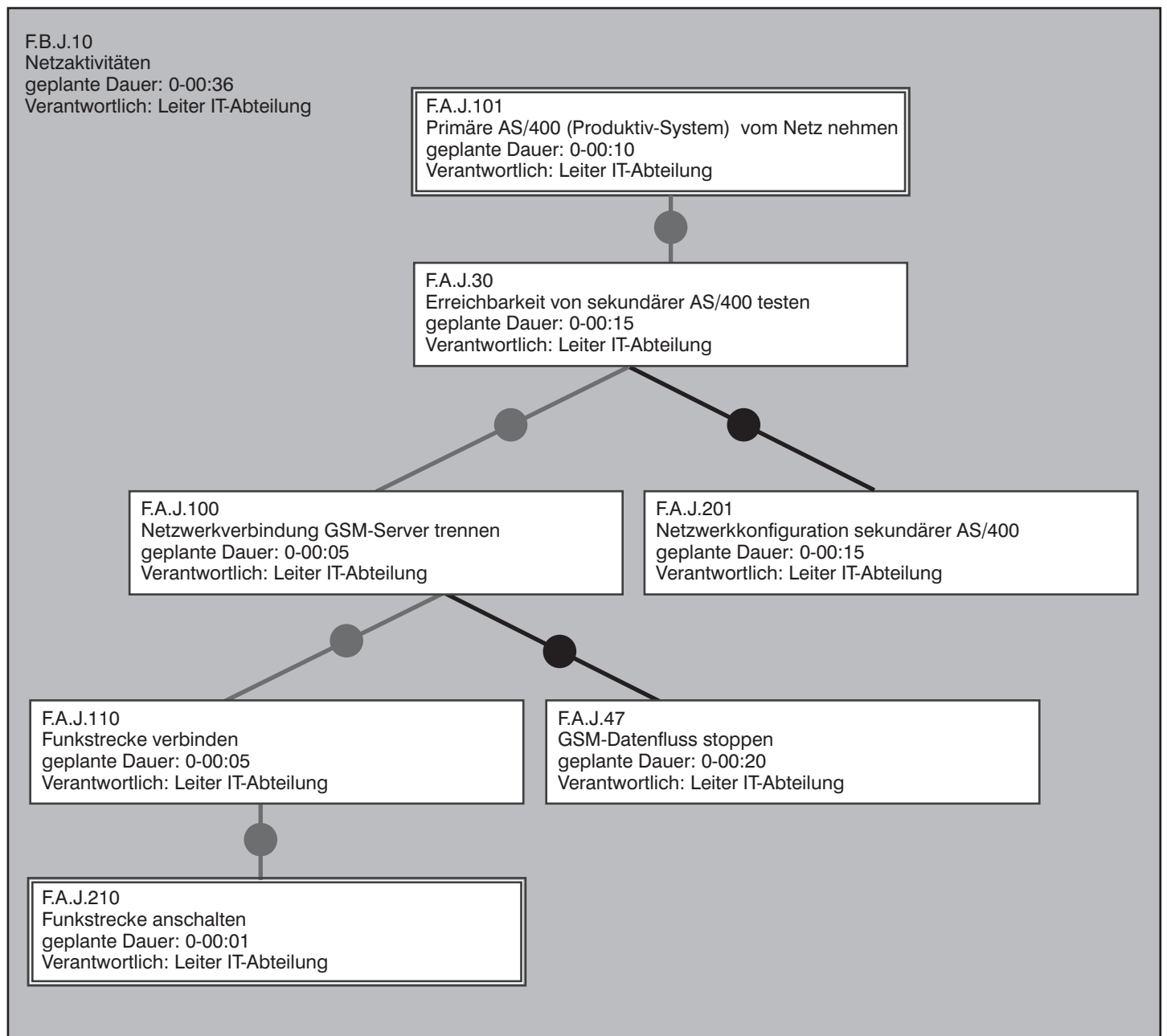


Abbildung 5: grafische Darstellung eines modularen Planungsblocks

Business Continuity Planning

herstellung notwendig wird oder wo diese stattfindet. Ursache und Wirkung müssen hier getrennt bleiben. Nur so können Planungsbestandteile modular in anderen Blöcken und Abläufen, wie zum Beispiel der Wiederherstellung des gesamten RZ an einem Ausweichstandort, eingesetzt werden. Abgesehen davon reduziert sich hierbei auch der Pflegeaufwand.

Die Gesamtheit der Notfallpläne sollte sowohl spezifische Wiederherstellungsprozeduren (Server, Netzwerkknoten, MVRZ) umfassen, als auch solche, die auf bestimmte Schadensereignisse, wie Hochwasser oder die Abtrennung von Gebäudeteilen, ausgerichtet sind.

Ist die Planung abgeschlossen, werden alle gewonnenen Informationen in einem Notfallhandbuch zusammengeführt. Folgende Angaben sollten dort in jedem Fall enthalten sein:

- Kurze Einleitung mit Zweck und den Aufbau des Dokumentes
- Darstellung der Notfallorganisation
- Krisenstäbe und Rollen der Mitarbeiter in den Krisenstäben
- Rufnummern- und Adresslisten von Mitarbeitern und Servicepartnern
- Übersichtliche Raum- und Gebäudepläne, Netzwerkstruktur, Adressräume usw.
- Kurze System- und Anwendungsbeschreibungen
- Grafische Darstellung von Systemabhängigkeiten
- Auflistung der definierten Notfälle

- Alarmierungsketten und Ablaufpläne

**Teststrategien**

Haben Sie in Ihrem Büro einen Feuerlöscher? Natürlich! Aber haben Sie jemals in Ihrem Leben schon mal einen bedient? Wissen Sie zum Beispiel, wie lange ein normaler Pulverlöscher funktioniert, bevor er leer ist? Im Ernstfall gibt es eben doch manchmal böse Überraschungen!

Ebenso verhält es sich mit Notfallhandbüchern. Prinzipiell ist immer alles klar, die Ablaufpläne theoretisch narrensicher. Beim initialen Test eines Notfallplanes zeigen sich jedoch (nach unserer Erfahrung) ausnahmslos immer noch kleine Unwägbarkeiten, die vorher nicht eingeplant wurden. Daher gilt ein Notfallplan auch nie als einsatzbereit, solange er nicht getestet wurde.

Für ein Notfallkonzept ist parallel daher auch immer ein Testkonzept zu entwickeln. Dabei werden, angepasst an die Art der Notfallpläne und die Wichtigkeit der dadurch abgesicherten Geschäftsprozesse, verschiedene Testabläufe festgelegt. Diese reichen vom einfachen „geistigen Durchgehen“ der Pläne bis hin zu einer realistischen Notfallübung mit einer tatsächlichen Unterbrechung des Produktivbetriebes. Dabei ist es offensichtlich, dass bei Tests der ersten Kategorie der Aufwand sehr gering ist und diese relativ häufig durchgeführt werden können, während ein wirklicher „Full Interruption Test“ wahrscheinlich nur sehr selten oder, realistisch gesehen, nie durchgeführt wird.

Die Teststrategie zur Notfallplanung legt nun fest, wie häufig welche Tests mit welchen Beteiligten durchzuführen sind. Dadurch werden sowohl die Pläne auf ihre Gültigkeit hin geprüft, als auch die Beteiligten geschult. Die Ergebnisse solcher Tests fließen wiederum in die Korrektur der Notfallplanung ein. Die nachstehende Tabelle gibt einen Überblick über verschiedene Testmethoden und ihren Aufwand. (siehe Tabelle 2)

Die Durchführung von Tests ist dabei nicht nur in starren zeitlichen Intervallen vorzusehen. Die Wirksamkeit von Notfallplänen lässt sich am besten durch unangekündigte Übungen überprüfen. Zusätzlich sollte ein außerplanmäßiger Test eingeschoben werden, wenn:

- neue Pläne erstellt wurden
- wesentliche Bestandteile der Planung geändert wurden
- neue Mitarbeiter den Notfallplan noch nicht kennen
- neue externe Dienstleister eingebunden werden
- Änderungen an Hard- und Software vorgenommen wurden
- eine neue Risikosituation Gewissheit über die Gültigkeit der Pläne erforderlich macht

**Phase 4: Wartung und Betrieb**

Wir sind am Ende des BCP „Projektes“ angekommen. Ab jetzt muss sich zeigen, ob die Vorbereitung in Phase 1 und die Kommunikation mit dem Management während des Projektes ausreichend war,

Bezeichnung	Inhalt	Beteiligte	Frequenz	Aufwand
Checklist Test	Der BCP-Verantwortliche jeder Abteilung geht für sich den Plan durch und überprüft ihn auf eventuelle Fehler oder Unzulänglichkeiten.	BCP-Verantwortlicher oder sein Team	↑ oft    selten	↓ gering    hoch
Structured Walk-Through Test	Alle Pläne werden gemeinsam an einem Tisch durchgearbeitet, um eventuelle Fehler in der Zusammenarbeit der Abteilungen aufzudecken (z.B. doppelte Verwendung von Ressourcen). Zusätzlich wird die Kommunikation zwischen den Teams getestet.	Alle BCP-Teams zusammen		
Simulation Test	Es werden alle Schritte von allen Beteiligten ausgeführt, wie sie im tatsächlichen Notfall geplant sind. Ausnahmen: Es werden keine Ersatzkomponenten geliefert (aber die Bestellung geprobt), es werden keine produktiven IT-Systeme modifiziert, es findet kein Umzug in einen Ausweichstandort statt. Es stehen nur die Ressourcen zur Verfügung, die im Notfall auch vorhanden wären.	Alle Mitarbeiter, die operationelle Aufgaben im BCP haben		
Parallel Test	Einrichtung des IT-Systems in einem Ersatzstandort. Dies kann eine MVRZ Übung oder die Verlagerung in ein Recovery Center sein	Alle Mitarbeiter, die operationelle Aufgaben im BCP haben sowie externe Dienstleister		
Full Interruption Test	Das Produktivsystem wird tatsächlich abgeschaltet und der Notfallplan durchgeführt	Alle Mitarbeiter sowie externe Dienstleister		

Tabelle 2: Gegenüberstellung der Teststrategien in Bezug auf Häufigkeit und Aufwand (nach PAS 56)

## Business Continuity Planning

um die Notfallplanung mit den nun notwendigen Ressourcen als Prozess weiter zu führen.

Regelmäßig wiederkehrende Tests und Reviews stellen die fortlaufende Aktualität und Anwendbarkeit der Notfallpläne sicher. Kennzeichnend für diese Phase ist auch die enge Integration in andere IT-Prozesse. Das Change Management ist hierbei am stärksten hervorzuheben. Das Notfallkonzept muss in den Change Management Prozess derart eingebunden werden, dass erfolgte Änderungen an der Systemumgebung umgehend in das Notfallkonzept eingearbeitet werden. Aber auch die Ergebnisse der BIA, ganz am Anfang des Projektes, sind nicht statisch. So werden sich ändernde Prämissen in den Geschäftsprozessen oder eine neue Risikosituation auch auf die dazugehörige Notfallplanung auswirken. Last but not least sind Schulungs- und Sensibilisierungsmaßnahmen der Mitarbeiter für ein lebendiges Notfallkonzept unabdingbar. In einem Notfall hat niemand die Zeit, zunächst ein dickes Handbuch zu studieren, dass er oder sie vorher nie gesehen hat.

### Einsatz von Tools

Das Notfallhandbuch mit allen wichtigen Informationen, Tabellen und Plänen zur Bewältigung von größeren Störfällen ist das wichtigste Ergebnis des Business Continuity Planning. Die Erstellung und Verwaltung von Notfallhandbüchern auf der Basis von reinen Office-Dokumenten ist jedoch aufgrund ihres großen Umfangs und der Komplexität sehr mühsam. Dass die gesamte Wartung und Pflege einer Notfallplanung oft unerledigt liegen bleibt, ist zum Teil auch durch hohen Aufwand begründet, den die ständige Aktualisierung der Dokumentation mit sich bringt. An dieser, aber auch an anderen Stellen, spielen die am Markt befindlichen Notfallplanungstools ihre Stärken aus. Folgende Aspekte sprechen für die Nutzung einer spezialisierten Software bei der Notfallplanung:

- Alle für den professionellen Einsatz relevanten Tools kennzeichnet die Nutzung einer internen Datenbank. Dadurch wird redundante Datenhaltung vermieden. Änderungen müssen nur an einer Stelle vorgenommen werden.
- In vielen Situationen wird es sinnvoll sein, wo überall und in welchen Handbüchern eine bestimmte Adresse oder ein bestimmter Ablauf verwendet wird. Entsprechende Software erspart Ihnen hier die mühselige Volltextsuche in allen Dokumenten.

- Die Rückverfolgbarkeit von Änderungen wird wesentlich erleichtert.
- Die Vergabe von Zugriffsrechten kann bis auf die Ebene einzelner Datensätze eingeschränkt werden, während bei der Version mit Office-Dokumenten nur ein Zugriffsschutz auf Dateiebene möglich ist.
- Oft werden mehrere Personen gleichzeitig am Notfallhandbuch arbeiten wollen. Ein Handbuch, das aus Office-Dokumenten besteht, ermöglicht das nicht.
- Bestehende Daten, zum Beispiel das Inventar von IT-Systemen, können bei den meisten Systemen problemlos importiert werden.
- Eine ansprechende grafische Präsentation der Ablaufpläne wird automatisch erstellt und muss nicht gezeichnet werden.
- Einige Tools bieten auch die Begleitung und Protokollierung von Tests, so dass deren Ergebnisse sofort in die Planung aufgenommen werden können.

Ein Tool, das auf Knopfdruck Notfallhandbücher schreibt, gibt es hingegen nicht. Die Verantwortung für eine vorausschauende Planung wird immer bei den BCP-Verantwortlichen bleiben.

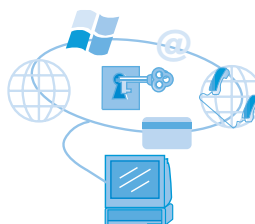
Es werden derzeit eine Reihe von Tools in diesem Segment am Markt angeboten. Wichtige Beispiele sind das Produkt

LDRPS von Strohl Systems, ROGSI/DMS von ROG, CAPT/CM von Heine & Partner sowie „alive-IT“ von Controll-IT. Die Screenshots in diesem Artikel stammen aus letzterem Tool.

### Fazit

Die Maßnahmen zur Notfallvorsorge, vor allem im IT-Bereich, haben lange Zeit ein eher stiefmütterliches Dasein gefristet. Teilweise wurde der Beitrag der IT zu den Geschäftsprozessen eines Unternehmens unterschätzt oder aber die vollständige Abhängigkeit von ihr ohne Sicherungsseil in Kauf genommen. Das ständig latente Risiko einer größeren Betriebsunterbrechung konnte den fehlenden gesetzlichen Zugzwang und die Sorge vor den Kosten eines Notfallkonzeptes nicht ausgleichen. In den letzten Jahren holt hier das Bewusstsein der Unternehmer langsam auf. Auch der Gesetzgeber und Branchenverbände legen nach und fordern in immer mehr Verordnungen eine angemessene Vorbereitung auf solche Ereignisse. Das wachsende KnowHow auf dem Gebiet der Notfallplanung, die steigende Zahl von Anbietern mobiler oder stationärer Ausweichstandorte und auch die fortschreitende Standardisierung erleichtern zunehmend die Umsetzung eines wirksamen und effektiven Notfallkonzeptes.

## IT-Sicherheits-Forum 2006



**08.05. - 11.05.06**  
in Bad Neuenahr

**Jetzt mit weiterem Workshop!!**

Am dritten Tag haben Sie am Vor- und Nachmittag je 4 Workshops zur Auswahl:

### Vormittag

- Workshop 1: Einsatz von netzwerk-basierten IPS
- Workshop 2: Modern Hacking - Know your Enemy - Live-Demo von Angriffstechniken
- Workshop 3: Business Continuity Planing im IT-Umfeld - Live-Demo eines Tools
- Workshop 4: Sicherheit von BlackBerry und Alternativlösungen - Vergleich unterschiedlicher Lösungen

### Nachmittag

- Workshop 5: IT-Security Best Practice - Top-10 Tips und Tricks in der Diskussion
- Workshop 6: Intelligente Analyse von Security Log Files
- Workshop 7: User Identity based access control- Zugriffsschutz auf allen Ebenen
- Workshop 3: Business Continuity Planing im IT-Umfeld - Live-Demo eines Tools

Moderation: Dipl.-Inform. Detlef Weidenhammer

Preis: € 2.190,- zzgl. MwSt. (4 Tage) bzw. € 1.790,- zzgl. MwSt. (3 Tage)



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

# Neuerscheinung März 2006

## Sicherheit in Enterprise-Netzen durch den Einsatz von 802.1X

Sie erhalten mit diesem Report ein umfassendes Grundlagenwerk, das Sie bei der Auswahl und beim Aufbau einer 802.1X-basierende Sicherheitslösung unterstützt, auf die verborgenen Fallstricke dieses Frameworks aufmerksam macht und wesentliche Betriebsaspekte offen legt.

Im Folgenden stellen wir Ihnen einen Auszug als Leseprobe zur Verfügung:

### 1.1 Auswahl der Authentifizierungsmethoden

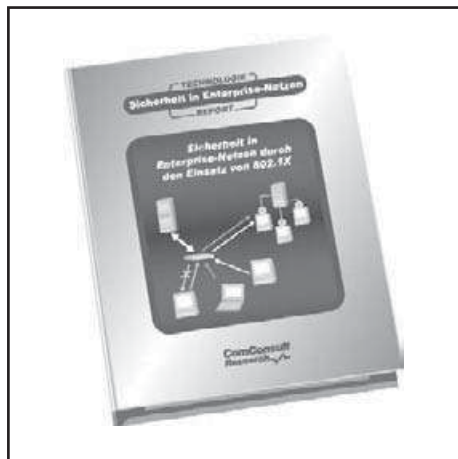
Bei der Wahl der EAP-Methode(n) sind im Wesentlichen die folgenden Punkte zu beachten:

- Welche Clients sollen unterstützt werden?
  - Geräte- oder Benutzerauthentifizierung?
- In welche Betriebssystem-Landschaft soll die Lösung integriert werden?
- Steht eine PKI zur Verfügung oder soll eine aufgebaut werden?
  - Falls Ja, sollen/können die Clients mit Zertifikaten ausgestattet werden oder nur die Authentifizierungsserver?
  - Falls alle oder auch nur einige Clients keine Zertifikate erhalten, gegen welche Datenbasis soll dann authentifiziert werden?
- Soll die Anbindung von Clients über Wireless LAN unterstützt werden?

#### 1.1.1 Geräte- oder Benutzerauthentifizierung

Die in Kapitel 3 vorgestellten Standards unterscheiden nicht zwischen Geräte- und Benutzerauthentifizierung. Tatsächlich ist diese Unterscheidung auch etwas akademisch, die beiden Begriffe stammen ursprünglich aus der Windows-Welt, wo im Active Directory Benutzerkonten und Computerkonten geführt werden. Eine Authentifizierung kann hier folglich gegen ein Benutzerkonto (= Benutzerauthentifizierung) oder gegen ein Computerkonto (= Geräteauthentifizierung) erfolgen.

Der entscheidende Unterschied zwischen beiden Authentifizierungstypen ist also nicht die Frage, welcher Kontentyp genutzt wird, sondern: Erfolgt die Authentifizierung mit oder ohne Interaktion mit einem Benutzer?



Unter Geräteauthentifizierung versteht man also einen Authentifizierungsvorgang, der ohne Eingaben von Benutzerseite automatisiert abläuft. In diesem Fall müssen die benötigten Authentifizierungsdaten (Credentials) folglich auf dem System lokal vorliegen.

Hiermit stellt sich unmittelbar die Frage nach der Sicherheit

1. für die hinterlegten Credentials auf dem Gerät und
2. für das zu schützende Netzwerk.

Bei Benutzerauthentifizierungen setzt man meist auf die Komponente „Wissen“ (in der Regel ein Passwort) oder auf eine Kombination aus den Komponenten „Wissen“ und „Besitz“ (z.B. Smartcard plus PIN), anhand derer der Benutzer identifiziert wird. Beides geht bei der Geräteauthentifizierung natürlich nicht, das Gerät identifiziert sich eben allein, Passwort oder Zertifikat sind direkt auf dem Gerät hinterlegt. Daher muss sichergestellt werden, dass diese Daten (Credentials) nicht entwendet und von anderen Systemen für einen unberechtigten Netzzugang missbraucht werden können.

Von den in Kapitel 3 vorgestellten EAP-Methoden nutzen die meisten ein Passwort zur Clientauthentifizierung und benötigen daher die Interaktion mit einem Benutzer – zumindest wenn man das Passwort nicht im Klartext auf dem Client hinterlegen möchte. Doch selbst wenn man sich dafür entscheiden würde, müssen für diese Verfahren gerätespezifische „Benut-

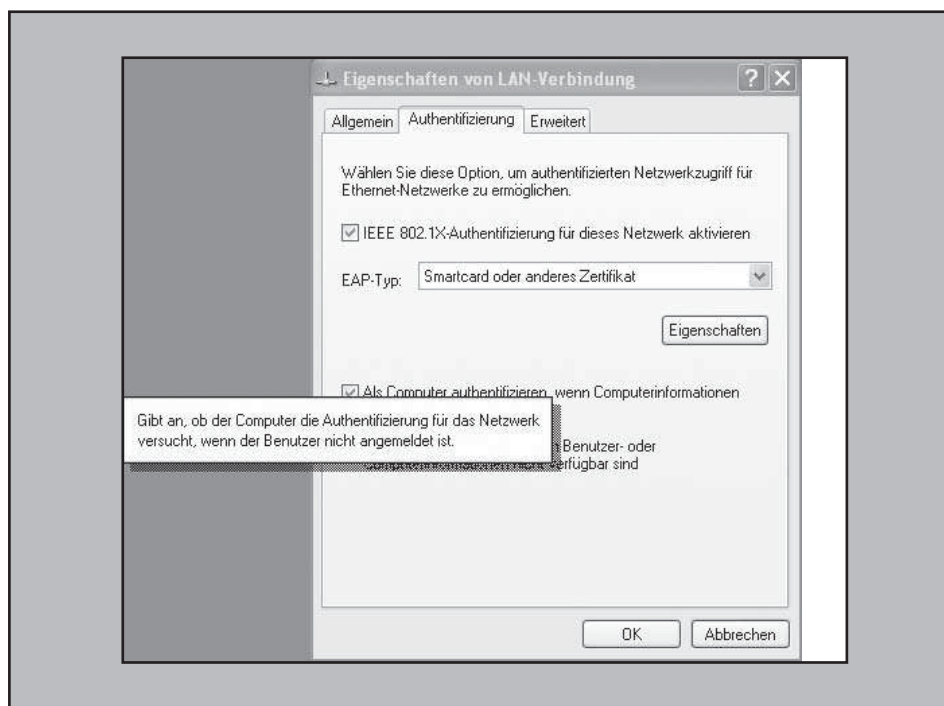


Abbildung 4.1: Aktivierung der Geräteauthentifizierung unter Windows XP

## Sicherheit in Enterprise-Netzen durch den Einsatz von 802.1X

zer“-Konten mit eigenen Passwörtern angelegt und gepflegt werden.

Ausnahmen und daher besser zur Geräteauthentifizierung geeignet sind:

- EAP-TLS, hierbei werden Clientzertifikate überprüft;
- EAP-FAST, hierbei wird ein Pre-Shared Key genutzt;
- EAP-SIM und EAP-AKA, hierbei werden Daten von SIM-Karten genutzt - dies setzt jedoch voraus, dass die SIM-Karten ohne PIN aktiviert werden können.

Zur Geräteauthentifizierung ist es also (selbstverständlich) erforderlich, dass der Authentication Server das Gerät über die gewählte EAP-Methode überhaupt authentifizieren kann! Das heißt, er muss je nach EAP-Methode auch über eine geeignete Datenbasis der Systeme verfügen.

Entscheidend, ob man sich für die Benutzer- oder Geräteauthentifizierung entscheidet, ist aber zunächst die Frage, wann das einzelne System Netzwerkzugriff benötigt: Bevor oder erst nachdem sich ein Benutzer angemeldet hat. Beispiele für einen Netzwerkzugriff ohne angemeldeten Benutzer sind:

- Wake-on-LAN,
- Softwareverteilungsroutinen,
- computerbasierte Richtlinien im Windowsnetz,
- lokale Ressourcen (wie z.B. Drucker), die im Netz freigegeben sind,
- zentrale Datensicherung lokaler Ressourcen,
- Serverdienste für das Netzwerk,
- öffentliche Angebote zur anonymen Nutzung wie beispielsweise ein Besucherinformationssystem an öffentlich zugänglichen PCs.

Darüber hinaus wird man schnell feststellen, dass es eine große Menge weiterer Geräte im Netzwerk gibt, die gar keine benutzerbasierte Authentifizierung sinnvoll zulassen. Hierzu gehören

- alle Server,
- Netzwerkdrucker,
- VoIP-Hardphones,
- Erfassungsgeräte wie Scanner, Zeiterfassungsterminals,
- Überwachungsgeräte wie Kameras,
- Steuerungstechnik,
- Produktionsmaschinen
- und viele mehr.

Zusammenfassend kann man über eine Geräteauthentifizierung sagen:

- Für eine flächendeckende Sicherheitslösung kann man in der Regel auf ge-

rätebasierende Authentifizierungsverfahren nicht verzichten.

- Zu prüfen ist dann, wie die Vorteile einer ergänzende Benutzerauthentifizierung integriert werden können (siehe hierzu Kapitel 4.1.3).
- Wünschenswert sind Geräteauthentifizierungen über EAP-TLS.

### 1.1.2 Authentifizierung auf Basis der MAC-Adresse

Falls von bestimmten Clienttypen keine 802.1X-basierende Authentifizierung unterstützt wird, müssen hierfür am Zugangspunkt/Switch Ausnahmeregelungen geschaffen werden, die letztlich Löcher in den aufgebauten Schutzwall reißen.

Als Authentifizierungsverfahren auf niedrigster Stufe bieten für diesen Fall die meisten Produkten an, auf der Basis von MAC-Adressen zu authentifizieren. Auch hierbei unterstützen die meisten Switches und Access Point neben der Definition einer lokalen Accessliste auch die Möglichkeit, die MAC-Adressen über RADIUS von einem zentralen Authentifizierungsserver überprüfen zu lassen. Damit verliert man zumindest den Vorteil der zentralen Datenbasis nicht, das Verfahren kann nahtlos in eine RADIUS-Infrastruktur zur Authentifizierung eingebettet werden und eignet sich daher insbesondere als Einstiegs- oder Übergangsvariante bei der Einführung von 802.1X.

Insbesondere alle über RADIUS austauschbaren Informationen (siehe Kapitel 4.3) können vom Switch/Access Point und vom Authentifizierungsserver übermittelt und ausgewertet werden.

Offensichtlich ist jedoch das Authentifizierungskriterium „MAC-Adresse“ kein geheimes Credential und kann daher leicht für Angriffe unter der Identität eines regulären Systems genutzt werden (MAC-Address-Spoofing). Dies ist das größte Problem an einer Authentifizierung via MAC-Adresse.

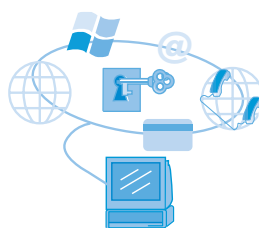
Zu beachten ist daher: Eine Authentifizierung über MAC-Adressen liefert zwar ein Accounting regulärer Benutzer bzw. Geräte und kann auch zur Trennung von Benutzergruppen verwendet werden, bietet aber für das entsprechende LAN-Segment keinen weiteren Schutz vor aktiven Angriffen!

Einige Produkte unterstützen pro Port eine Art Fall-Back der Authentifizierungsverfahren:

- Als Erstes wird über EAP-Request-Identity eine 802.1X-Authentifizierung gestartet,
- wird dieser Request innerhalb eines Timeout-Intervalls nicht beantwortet, wird (über RADIUS) versucht die MAC-Adresse zu überprüfen.

Eine solche sich automatisch zurückstufende Authentifizierung mag während ei-

## 15% Rabatt bei Kongressteilnahme



Als Teilnehmer am

### IT-Sicherheits-Forum

**08.05. - 11.05.06**

haben Sie die Möglichkeit, den Report stark reduziert zu erwerben.

Das IT-Sicherheits-Forum 2006 wird auch in diesem Jahr wieder die gerade aktuellen Themen zu Bedrohungsszenarien der IT-Sicherheit und zu den wichtigsten Schutzmaßnahmen aufgreifen. Dabei wird ein äußerst großer Wert auf Praxisnähe gelegt, dies zeigt sich insbesondere bei den technisch orientierten Workshops und den Praxisvorträgen, die direkt anwendbare „Tipps & Tricks“ für den Tagesbetrieb weitergeben.

Das Forum hat sich deshalb in den letzten Jahren zu einem stark besuchten Treffpunkt für alle Sicherheitsinteressierten entwickelt. An insgesamt vier Tagen werden angeboten:

- Erfahrungen aus aktuellen Sicherheitsvorfällen und Aufzeigen absehbarer Trends
- Neue Entwicklungen bei Sicherheitstechnologie und Sicherheitsorganisation
- Moderierte Workshops mit Produktvergleichen und Live-Demos
- Vertiefende Seminare und Tutorien

Moderation: Dipl.-Inform. Detlef Weidenhammer

Preis: € 2.190,- zzgl. MwSt. (4 Tage) bzw. € 1.790,- zzgl. MwSt. (3 Tage)



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

Sicherheit in Enterprise-Netzen durch den Einsatz von 802.1X

ner Umstellungsphase hilfreich sein, ist aber sicherheitstechnisch zunächst nicht besser als eine MAC-Adressen-basierende Authentifizierung.

Hilfreich ist jedoch das folgende Szenario (siehe auch Abbildung 4.3): Alle über MAC-Adresse authentifizierten Geräte werden dynamisch einem separaten VLAN zugeordnet, welches höheren Sicherheitsbeschränkungen unterworfen ist und durch eine Firewall von restlichen LAN getrennt ist. Aber auch hierbei ist zu bedenken, dass damit alle Systeme in diesem VLAN untereinander nicht geschützt sind und dass es außerdem Angriffsszenarien gibt, die in der Lage sind VLAN-Grenzen zu überschreiten (VLAN-Hopping).

In jedem Fall sollte jedoch für LAN/WLAN-Segmente, in denen Wireless Clients eingesetzt werden müssen, die kein WPA oder 802.11i unterstützen und daher per MAC-Adresse authentifiziert werden, notwendigerweise ein eigenes isoliertes Netzsegment geschaffen werden, welches den gesamten Netzverkehr über eine geeignete Firewall leitet. Zu beachten ist hierbei außerdem, dass ohne WPA/802.11i auch keine sichere Verschlüsselung der übertragenen Daten gewährleistet ist!

Für Wireless LANs nach 802.11i fordert der Standard die Unterstützung dynamischer Schlüsselaustauschverfahren, wo-

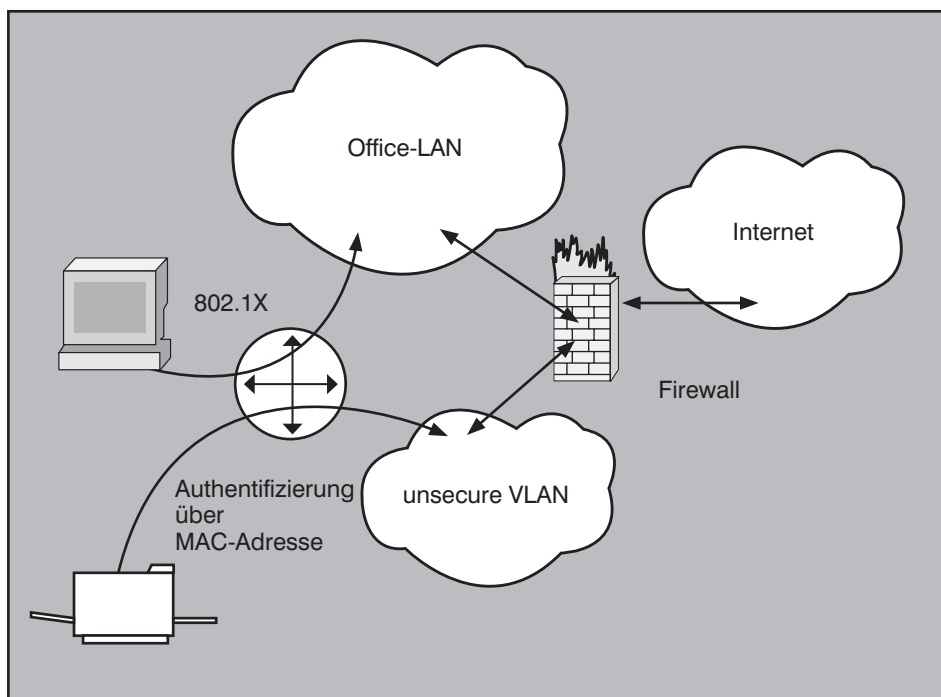


Abbildung 4.3: Trennung von sicher und unsicher authentifizierten Geräten

bei der PMK (siehe Kapitel 0) jedoch nicht notwendigerweise von einem EAP-Verfahren geliefert werden muss, sondern bei reduziertem Schutzbedarf auch als Pre-Shared Key fest vorgegeben werden kann. Dieses oft als WPA-PSK bezeichnete Verfahren liefert ein akzeptables Sicher-

heitsniveau, falls der Pre-Shared Key genügend komplex gewählt ist (mindestens 20 zufällige Zeichen), und kann durch die zusätzliche Überprüfung der MAC-Adressen ergänzt werden.

Fax-Antwort an ComConsult 02408/955-399

# Bestellung

## Sicherheit in Enterprise-Netzen durch den Einsatz von 802.1X

Ich bestelle den Report **Sicherheit in Enterprise-Netzen durch den Einsatz von 802.1X** (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)

Neues Seminar

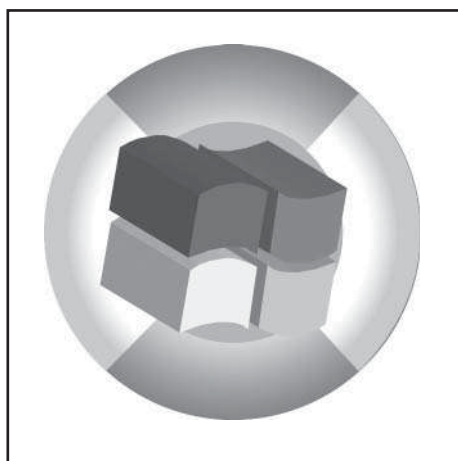
# Troubleshooting Windows Server 2003 Active Directory

Die ComConsult Akademie veranstaltet vom 15. - 17. Mai erstmalig ihr neues Seminar „Troubleshooting Windows Server 2003 Active Directory“ in Aachen.

Das 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.

Auch mit der deutlich verbesserten Version 2 des Active Directory ist die Implementierung weiter sehr komplex. Dementsprechend häufig sind Konfigurationsfehler und Probleme im Betrieb. Dieses 3-tägige Seminar befasst sich mit der Vermeidung und Handhabung von Fehlersituationen in der Nutzung von Active Directory.

Thematisch unterteilt sich das Seminar in die Schwerpunkte: Active Directory (AD) Backup/Restore, Distributed File System (DFS - inkl. Neuerungen aus Release 2), Low-Level „Manipulation“ des AD, LDAP-Zugriffe, AD und Netzwerk, AD und IP-Management, AD Replikation, AD Standorte, AD und Gruppenrichtlinien.



Das Seminar richtet sich in erster Linie an Betreiber und Administratoren, die das Active Directory einsetzen. Ferner richtet es sich auch an Planer, die im Vorfeld aufgrund von Praxiserfahrungen Fehler vermeiden möchten. Grundvoraussetzung sind Kenntnisse im Bereich des Active Directory und des IP-Managements, so wie im Report zu Windows Server 2003 Active Directory und IP-Management dokumentiert.

Auf diesem Seminar lernen Sie:

- Grundsätzlicher Umgang mit Problemen im Bereich des Active Directory
- Das Backup und Restore des Active Directory in verschiedenen Situationen
- Low-Level „Manipulation“ des Active Directory zur Fehlerbeseitigung
- Fehlerbeseitigung im Bereich des grundlegenden IP-Managements und des Netzwerks
- Optimierung im Bereich der Active Directory Replikation und der Standorte zur Fehlerbeseitigung und zur Fehlervermeidung
- Richtiger Umgang mit Gruppenrichtlinien und die Bereinigung von Fehlern in diesem Themenkomplex
- Vermeidung von Fehlern im Bereich des Distributed File System und Vorstellung der Verbesserung im neuen DFS des Release 2 von Windows Server 2003
- Fehlerbeseitigung und -vermeidung in weiteren Detailthemen wie Drucker, Vertrauensstellungen - insbesondere zu anderen Welten, Zeitsynchronisation und FSMO-Rollen

Durch das Seminar führen Sie: Dipl.-Geol. Martin Gödde, Markus Holländer, Dipl.-Ing. Lars Kuhl, Dipl.-Inform. Michael van Laak, Frank Neunzig, Dipl.-Ing. Rainer Schüer von der ComConsult Beratung und Planung GmbH.


Fax-Antwort an ComConsult 02408/955-399

## Anmeldung

# Troubleshooting Windows Server 2003 Active Directory

Ich buche das Seminar **Troubleshooting Windows Server 2003 Active Directory** vom 15. - 17.05.06 in Aachen zum Preis von € 1.690,- zzgl. MwSt.

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

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

Vorname \_\_\_\_\_ Nachname \_\_\_\_\_

Firma \_\_\_\_\_ Telefon/Fax \_\_\_\_\_

Straße \_\_\_\_\_ PLZ, Ort \_\_\_\_\_

eMail \_\_\_\_\_ Unterschrift \_\_\_\_\_

Schwerpunktthema

# Troubleshooting Windows Server 2003 Active Directory - oft eine komplexe Sache!

Fortsetzung von Seite 1



Markus Holländer ist Competence Center Leiter Backoffice bei der ComConsult Beratung und Planung GmbH. Neben der Leitung des Competence Centers sind seine Hauptaktivitäten Projektleitungen, Konzipierungen und Reviews im Bereich der Themen Windows Server 2003 (2000), Active Directory, DNS und Windows XP für private und öffentliche Auftraggeber. Insbesondere zu diesen Themenkomplexen verfügt er über jahrelange Projekterfahrung bei namhaften Unternehmen und eine Vielzahl erfolgreich abgeschlossener Projekte. Herr Holländer ist auch für die Entwicklung der Windows Server 2003 Seminare des Competence Centers in Zusammenarbeit mit der ComConsult Akademie verantwortlich und einer der Hauptreferenten.

Im Folgenden werden einige Szenarien beschrieben. Die anonymisierten Informationen hierzu stammen in der Regel aus realen Projekten und wurden ggf. teilweise für diesen Artikel angepasst. Zu Beginn wird „das Pferd mal von hinten“ aufgezümt und es wird mit folgendem Szenario gestartet:

### Domänenkontroller ist unwiederbringlich ausgefallen

Man stelle sich folgendes Szenario vor: Ein entscheidender Domänenkontroller ist durch einen Hardwaredefekt unwiederbringlich ausgefallen. Entscheidend ist dieser Domänenkontroller, weil er ebenfalls noch der so genannte „PDC-Emulator“ der Domäne ist. Der „PDC-Emulator“ oder auch „PDC-Advertiser“ ist eine FSMO- (Flexible Single Master Operation) Rolle, die nur ein Domänenkontroller innehaben kann. Natürlich kann diese Rolle, wie bei allen anderen FSMO-Rollen auch, verschoben werden, aber prinzipiell bzw. „by design“ ist es so, dass nur ein Domänenkontroller diese Funktionalität beheimatet. Der „PDC-Emulator“ stellt, wie der Name schon sagt, einen PDC (Primary Domain Controller) für NT-Rechner/-Benutzer zur Verfügung. Er ist aber auch beispielsweise der zentrale Zeitgeber in der Active Directory Domäne bzw. wenn es sich um den PDC-Emulator der Active Directory Root Domäne handelt, sogar in der Gesamtstruktur. Auch ist er der Standardserver zur Bearbeitung von Gruppenrichtlinienobjekten eine Funktion, die ggf. öfters benötigt wird. Aber um zurück auf das Szenario zu kommen: er hat mit dieser FSMO-Rolle eine entscheidende Funktionalität, und diese Funktionalität steht neben den „Standardfunktionen“ eines Domänenkontrollers (z.B. Authentifizierung) nicht mehr zur Verfügung. Der Ausfall der Standardfunktionen wird bei

entsprechendem Design von anderen Domänenkontrollern automatisch aufgefangen, der Ausfall der FSMO Rolle(n) nicht. In diesem Fall bedeutete dies z.B., dass kein NT-User sein Kennwort ändern konnte und - eigentlich viel schlimmer -, dass die Zeit der verschiedenen Rechner auseinander lief. Wenn die lokale Zeitdifferenz der Systeme innerhalb einer Active Directory Domäne zu groß wird, ist keine Kerberos-Authentifizierung mehr möglich. Natürlich spielen noch weitere Dinge, wie beispielsweise der automatische Aufbau der Replikationstopologie eine Rolle, doch darauf wird hier nur am Rande eingegangen. Der Ausfall des Rechners fiel durch das normale Servermonitoring auf. In der Abbildung 1 sieht man den Server (NETSRV05 im nachgestellten Fall) korrekt laufend und den PDC Emulator ausführend

im Windows Server 2003 Tool „Replication Monitor“ (übrigens ein sehr zu empfehlendes Tool).

In der Abbildung 2 wird im „Replication Monitor“ angezeigt, dass auf den Domänenkontroller nicht mehr zugegriffen werden kann und dass die Replikationsverbindungen zu einem anderen Domänenkontroller (NETSRV06) nicht mehr zur Verfügung stehen. Schaut man aber in andere Verwaltungstools, wie z.B. unter „Standorte und Dienste“ bzw. „sites and services“, dann sieht man nicht auf den ersten Blick, dass der Domänenkontroller weg ist. Da man ja aber weiß, dass der Domänenkontroller nicht mehr da ist und auch nicht mehr gerettet werden kann, kommt man ggf. als erstes auf den Gedanken, diesen „einfach“ zu löschen, da

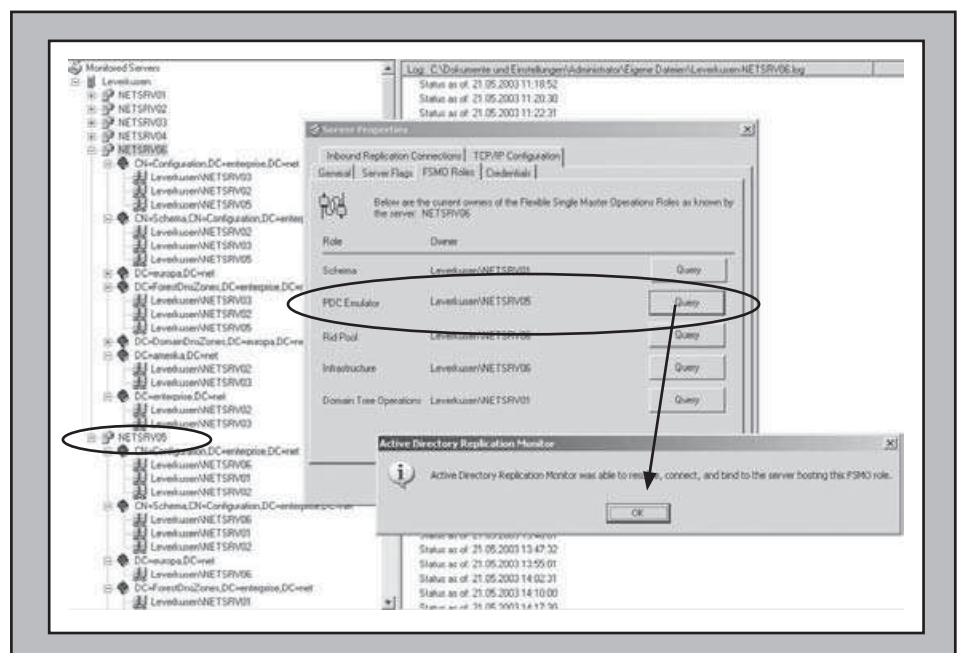


Abbildung 1: Ausfall eines Domänenkontrollers mit PDC-Emulator Funktion - noch alles in Ordnung

Troubleshooting Windows Server 2003 Active Directory - oft eine komplexe Sache!

dann - so der Gedanke - das Active Directory alles Notwendige macht. Hierzu geht man dann in das Active Directory MMC Snap-In „Benutzer und Computer“ in die Organisationseinheit „Domain Controllers“, macht einen Rechtsklick auf den entsprechenden Domänenkontroller und wählt „Löschen“. Nach der Sicherheitsabfrage erhält man dann eine weitere Abfrage, siehe Abbildung 3. Hier wählt man dann logischerweise die folgende Option: „Dieser Domänenkontroller ist permanent offline und kann nicht mehr mit dem Assistenten zum Installieren von Active Directory (DCPROMO) herabgestuft werden.“ Dies passt ja hundertprozentig zum Szenario und es sieht so aus, als würden alle Anforderungen erfüllt. Im Anschluss wählt man dann „Löschen“. Daraufhin erhält man eine weitere Sicherheitsabfrage, die einem nochmals mitteilt, dass das Objekt, welches man löschen möchte, ein Container ist und dass weitere Objekte enthalten sind. Dass man diese Objekte neben dem eigentlichen Objekt ebenfalls löschen möchte, bestätigt man dann nochmals. Im Anschluss ist der Domänenkontroller auch aus dem entsprechenden Container im Snap-In „Active Directory Benutzer und Computer“ verschwunden.

Insofern könnte man denken, dass schon alle notwendigen Schritte zur Entfernung des Domänenkontrollers durchgeführt seien, zumal ja explizit die Nachfrage kam, dass dies nicht mittels DCPROMO - also auf dem Standardweg - erfolgen kann. Eine erste Ernüchterung tritt ein, wenn man dann das Snap-In „Standorte und Dienste“ öffnet und darin noch den soeben gelöschten Server vorfindet. Wenn man jetzt davon ausgeht, dass dies ein Schönheitsfehler ist oder wie Microsoft so oft sagt „by design“, und möchte das Objekt auch in diesem Verwaltungstool löschen, wird man enttäuscht. Auch in diesem Fall kann man über Rechtsklick auf den entsprechenden Server im Kontextmenü die Option „Löschen“ wählen. Zuerst erhält man dann die Standard-Sicherheitsabfrage, ob man das Objekt löschen möchte. Nachdem man dies bestätigt hat, erhält man eine weitere Sicherheitsabfrage, nämlich genau die letzte Abfrage, die man auch beim Löschvorgang innerhalb von „Benutzer und Computer“ hatte. Bestätigt man auch diese und denkt, dass damit der Vorgang abgeschlossen ist, erhält man eine ernüchternde Fehlermeldung, siehe hierzu Abbildung 4.

Spätestens jetzt stellt man fest, dass man auf diesem Wege nicht weiter kommt und dass das richtige Troubleshooting beginnt. Wie im weiteren Verlauf zu sehen sein wird, werden ab diesem Zeitpunkt

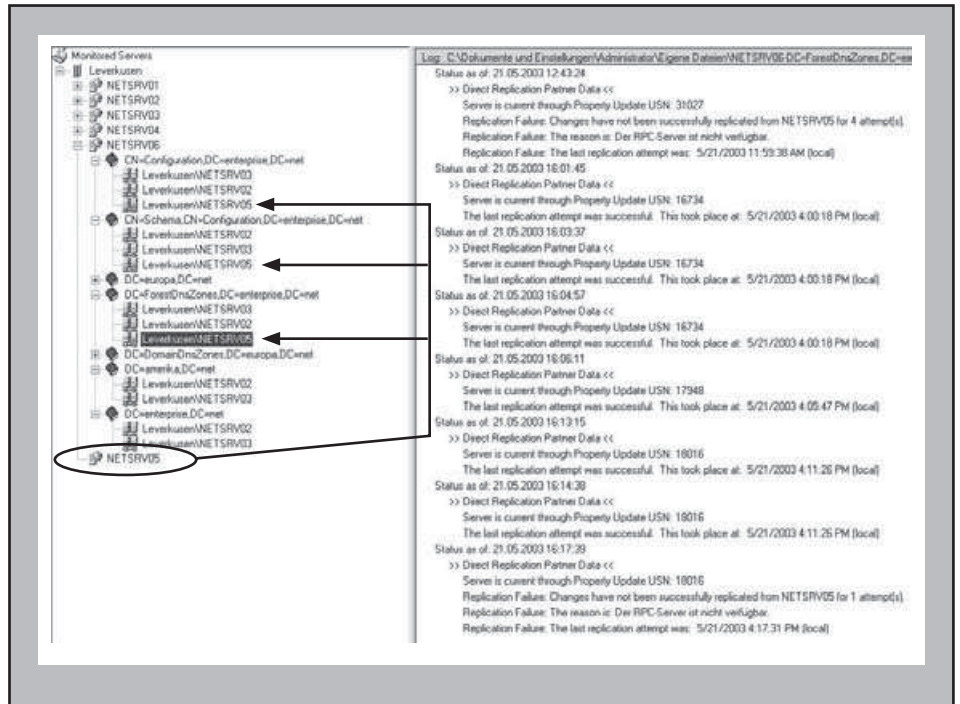


Abbildung 2: Ausfall eines Domänenkontrollers mit PDC-Emulator Funktion - DC steht nicht mehr zur Verfügung

verschiedene Low-Level-Tools benötigt und eingesetzt. Als erstes sollte man dafür sorgen, dass die FSMO-Rolle auf einen laufenden Server transferiert wird. Hierzu benötigt man dann „NTDSUTIL“, da der FSMO-Rollentransfer mittels GUI (Active Directory Benutzer und Computer) nur möglich ist, wenn der aktuelle Rolleninhaber online ist. In der Eingabeaufforderung startet man unter Eingabe von „ntdsutil“ das Werkzeug. Als nächstes gibt man „roles“ ein, da man eine FSMO-Rolle bearbeiten möchte. Dann tippt man „connections“ ein, um die Möglichkeit zu haben, sich mit

einem Domänenkontroller zu verbinden. Im Anschluss verbindet man sich unter Eingabe von „connect to server netsrv06.europa.net“ mit einem verbleibenden Domänenkontroller der Domäne (hierzu verwendet man den FQDN - hier im Beispiel „netsrv06.europa.net“). Nach erfolgreichem Verbinden mit dem Domänenkontroller muss man eine Ebene zurück, dies macht man unter Eingabe von „quit“. Anschließend gibt man „seize PDC“ ein, um die FSMO-Rolle PDC-Emulator auf den verbundenen Domänenkontroller zu verschieben. Nach einer Sicherheitsabfrage,

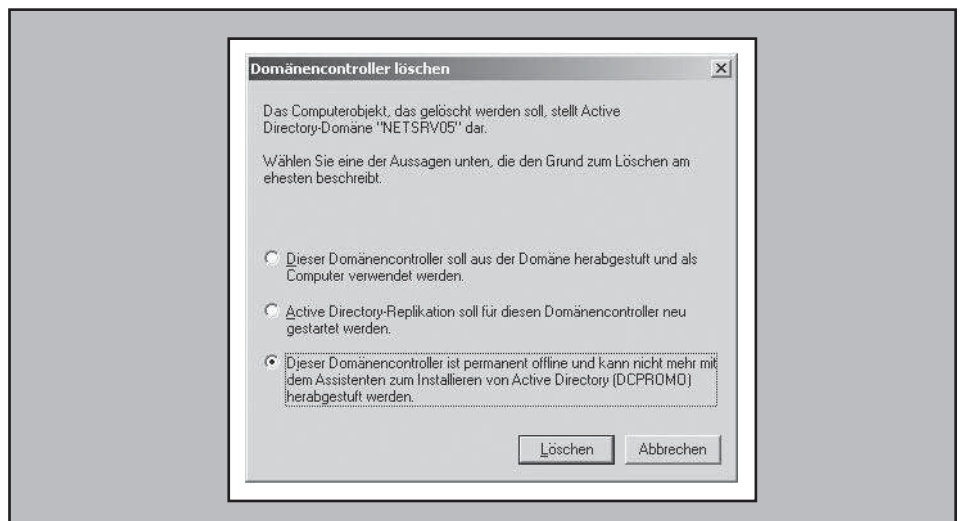


Abbildung 3: Sicherheitsabfrage beim Löschen des Computerobjekts

Troubleshooting Windows Server 2003 Active Directory - oft eine komplexe Sache!



Abbildung 4: Containerobjekt kann nicht gelöscht werden.

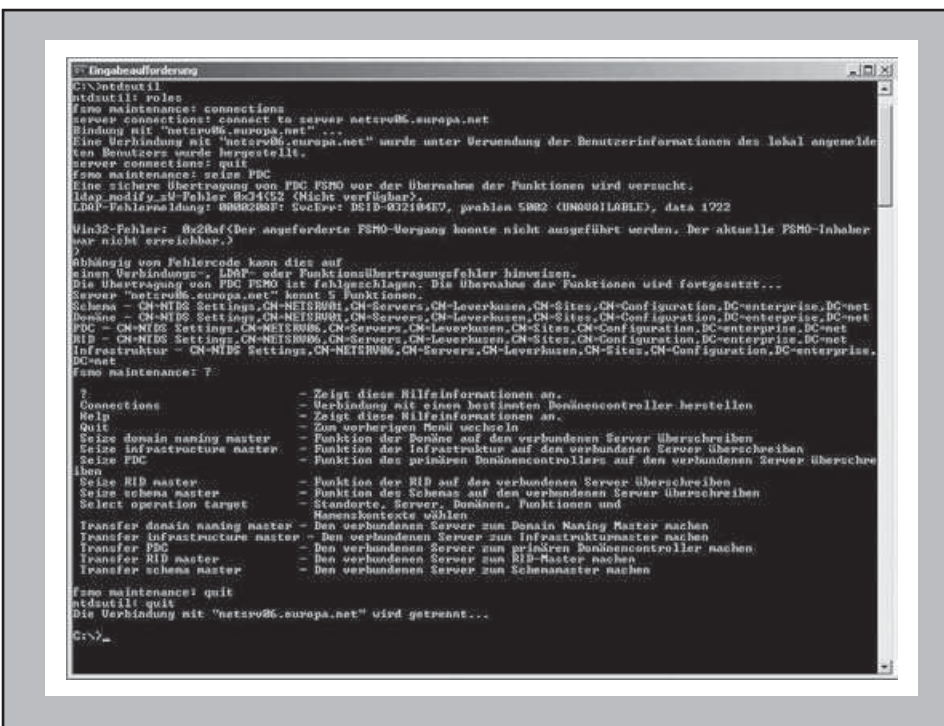


Abbildung 5: NTDSUTIL zum Verschieben der FSMO-Rolle

ob man die Rolle auch wirklich verschieben möchte, und diversen Überprüfungen wird die Rolle dann übertragen und

der gewählte Domänencontroller ist PDC-Emulator. Zum Beenden muss noch zweimal „quit“ eingegeben werden. Die soe-

ben beschriebenen Schritte sind auch der Abbildung 5 zu entnehmen.

Wenn man jetzt in den „Replication Monitor“ schaut, wird man feststellen, dass der PDC-Emulator verschoben wurde. Insofern wurde bereits die wichtigste Aktion durchgeführt und die „Dienste“, die nur der defekte Domänencontroller ausführte, werden jetzt von einem laufenden Domänencontroller bereitgestellt. Allerdings ist der defekte Domänencontroller immer noch im Verzeichnis vorhanden. Zur vollständigen Entfernung sind dann noch die folgenden Schritte erforderlich: Man startet den „Low Level Editor“ für das Active Directory „ADSI Edit“ (ein Support Tool für Windows Server 2003). Natürlich muss man unter Verwendung eines entsprechenden administrativen Accounts angemeldet sein. Da man Objekte/Attribute im so genannten „Configuration Naming Context“ bearbeiten bzw. löschen möchte, muss man sich mit einem Benutzer angemeldet haben, der Mitglied der „Enterprise Admins“ bzw. zu Deutsch der „Organisations-Admins“ ist. Im „Configuration Naming Context“ werden ja insbesondere die Informationen zu den Sites bzw. Standorten (inkl. Subnetze, Replikationsverbindungen, Domänencontroller), den vorhandenen Domänen und Trees (Struktur) im Forest (Gesamtstruktur), Vertrauensstellungen zu anderen Domänen sowie weitere globale Information alle Domänen einer Gesamtstruktur betreffend, gespeichert. Nach dem Start von „ADSI EDIT“ öffnet man als erstes den „Configuration Naming Context“ (im Szenario CN=Configuration,DC=enterprise,DC=net), dann „CN-Sites“, dann den entsprechenden Standort (in Szenario CN=Leverkusen) und zum Abschluss CN=Servers. Im Anschluss erhält man im Detailfenster auf der rechten Seite (siehe Abbildung 6) alle

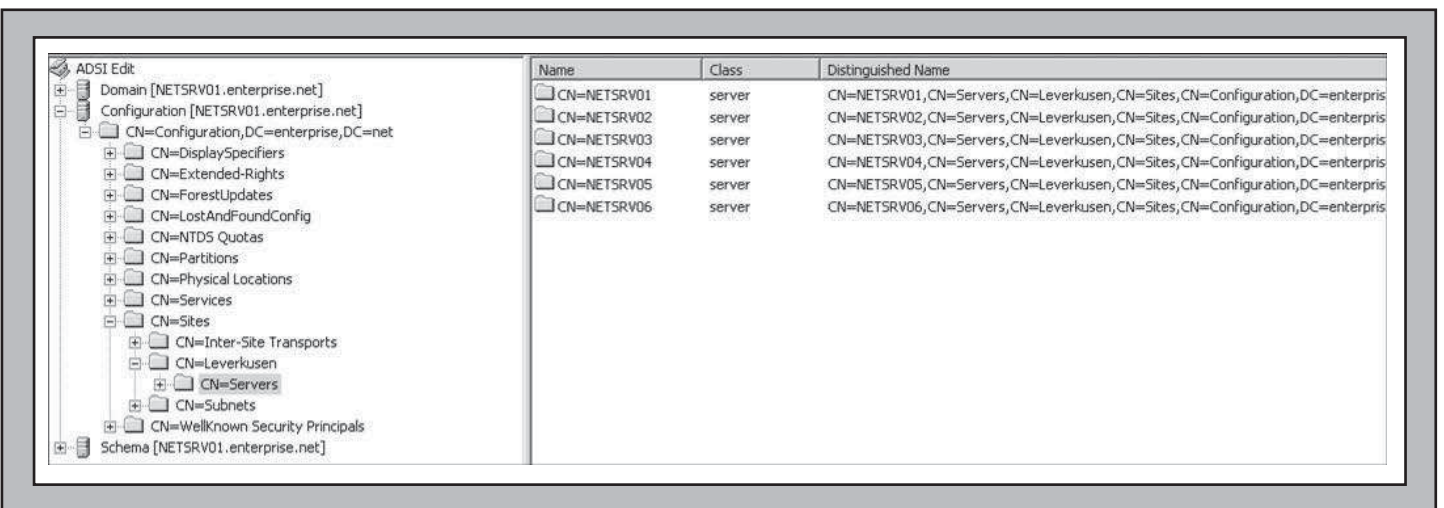


Abbildung 6: ADSI Edit für Aufräumarbeiten

## Troubleshooting Windows Server 2003 Active Directory - oft eine komplexe Sache!

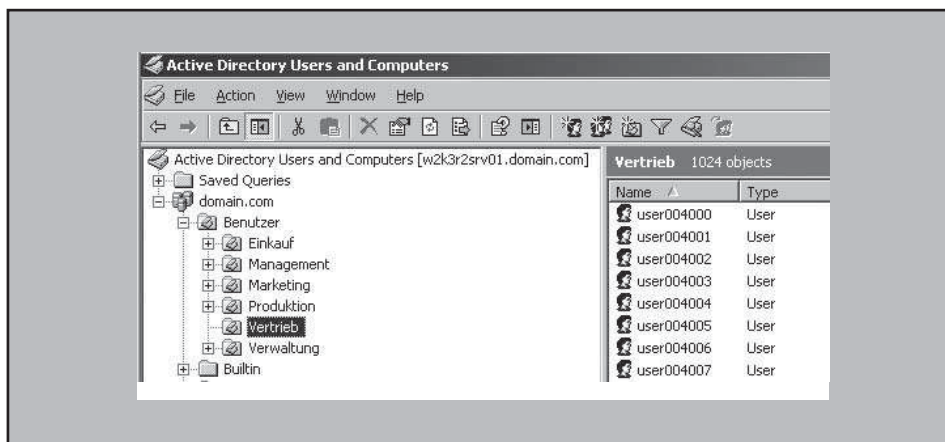


Abbildung 7: Organisationseinheit mit 1024 Benutzern

Server, die für diesen Standort (diese Site) konfiguriert sind. Mit Rechtsklick auf den zu löschenden Server (CN=NETSRV05) öffnet man das Kontextmenü, wo man den Eintrag „löschen“ wählt. Nach 2 zu bestätigenden Sicherheitsabfragen (einmal standard, ob man dies wirklich löschen möchte und einmal die Zusatzfrage, ob auch alles in diesem Container mitgelöscht werden kann) ist der Server dann aus dem „Configuration Naming Context“ verschwunden.

Wenn man jetzt die anderen Verwaltungstools (z.B. „Standorte und Dienste“ oder den „Replication Monitor“) öffnet, stellt man fest, dass der Server auch tatsächlich aus dem Verzeichnis entfernt wurde. Insofern können dann auch wieder alle automatischen Mechanismen, z.B. die Erstellung der Replikationstopologie und die Replikation selber, einwandfrei arbeiten. Eines sollte man jedoch nicht vergessen: die Überprüfung und Bereinigung im Umfeld der Namensauflösung. Hierzu sollte man sich DNS anschauen und bereinigen und ggf. die Service Records neu erzeugen lassen sowie auch WINS - sofern verwendet - bereinigen. Dieses Szenario zeigt schon ganz eindeutig, dass das Troubleshooting im Bereich des Active Directory nicht ganz trivial ist, dass man nicht nur mit den Standardverwaltungstools auskommt und spezielle Tools wie „ADSI Edit“ und „NTDS Util“ benötigt werden, und auch dass man sich im „Verzeichnis“ (FSMO-Rollen, Partitionen ...) auskennen muss. Man hat an diesem Szenario auch schon erahnen können, dass die benutzten Low-Level Tools ziemlich mächtig sind, so dass hier insbesondere darauf hingewiesen sei, dass fundierte Kenntnis erforderlich ist und die nötige Vorsicht absolut erforderlich ist! Im zuvor dargestellten Troubleshooting Szenario sollte das Verzeichnis bereinigt werden - der zweite Fall beschäftigt sich mit der Wiederherstellung von Informationen des Active Directory.

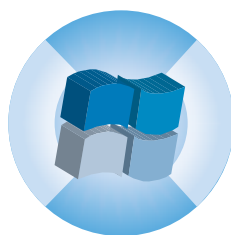
### Active Directory Backup und Wiederherstellung

Dies ist eigentlich ein ziemlich einfacher Fall: Ein Administrator hat eine vollständige Organisationseinheit (siehe Abbildung 7), in der sich Benutzer befinden - im nachgestellten Szenario für die Screenshots 1024 Benutzerkonten der Organisationseinheit „Vertrieb“, gelöscht. Der ein oder andere wird sagen, das kommt doch in der Praxis nicht vor, es gibt doch 2 Sicherheitsabfragen! Stimmt - die Sicherheitsabfragen kommen, doch es ist genauso wahr, dass es diese Fälle gibt bzw. gab, denn dies trat nicht nur einmal

auf. Noch ein Hinweis; das nachgestellte Szenario wurde in einer Umgebung mit Windows Server 2003 Service Pack 1 aufgebaut. Im Detail gibt es hier Unterschiede zu Umgebungen ohne Service Pack 1.

Vorweg noch eine ganz interessante Sache, die dem Einen oder Anderen sicher nicht so bewusst ist. Im Active Directory gibt es eine so genannte „tombstone-lifetime“ - wörtlich übersetzt die Lebenszeit des Grabsteins, wobei dies schon deutlich macht, worum es sich handelt. Wird ein Objekt im Active Directory gelöscht, dann wird es im ersten Schritt „nur“ als gelöscht markiert (tombstone) und nach x-Tagen (lifetime) dann endgültig aus dem Active Directory entfernt. Eigentlich gut so, sollte man denken, doch das wichtige ist, dass man für ein „authoritative restore“ (wie es für das geschilderte Szenario erforderlich ist) ein Backup benötigt, welches jünger als die „tombstone lifetime“ ist. Im Standard ist die „tombstone lifetime“ 60 Tage bei einem Forest (Gesamtstruktur), der mit Windows Server 2003 aufgesetzt wurde. Wurde oder wird jedoch der erste Domänencontroller der „Root Domain“ mit Windows Server 2003 Service Pack 1 aufgesetzt, so hat Microsoft die „tombstone lifetime“ auf 180 Tage verdreifacht (dies erfolgt nicht, wenn das Service Pack 1 nachträglich installiert wird!). Dies vergrößert dann auch den Spielraum für das Backup erheblich. Im Anhang unter „VBS Skript

## NEUE VERANSTALTUNG!



### Troubleshooting Windows Server 2003 Active Directory 15.05. - 17.05.06 in Aachen

Auch mit der deutlich verbesserten Version 2 des Active Directory ist die Implementierung weiter sehr komplex. Dementsprechend häufig sind Konfigurationsfehler und Probleme im Betrieb. Dieses 3-tägige Seminar befasst sich mit der Vermeidung und Handhabung von Fehlersituationen in der Nutzung von Active Directory.

Das 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.

Referenten: Markus Holländer, Dipl.-Inform. Michael van Laak, Frank Neunzig, Dipl.-Ing. Lars Kuhl, Dipl.-Ing. Rainer Schürer, Dipl.-Geo. Martin Götde, Peter Kleynen. Preis: € 1.690,- zzgl. MwSt.



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

## Troubleshooting Windows Server 2003 Active Directory - oft eine komplexe Sache!

zur tombstone lifetime“ ist ein Visual Basic Skript dargestellt, mit dem die „tombstone lifetime“ gesetzt werden kann. Die Abbildung 8 zeigt die Ausführung dieses Skripts. Auch ist in diesem Screenshot ein Befehl zum Check der „tombstone lifetime“ zu sehen: „dsquery \* „CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=domain,DC=com“ -scope base -attr tombstonelifetime“ (natürlich für das Beispielszenario mit der Domäne „domain.com“). Ergibt die Abfrage keinen Wert, so ist der Standard hinterlegt (60 oder 180 Tage).

Aus dem oben definierten Umstand lassen sich noch 2 wichtige Punkte ableiten: Zum einen sollte man also dafür sorgen, dass man ein möglichst aktuelles Backup des Active Directory hat, aus dem die wiederherzustellenden Objekte kommen. Grundsätzlich spricht wenig dagegen, dass auf ausgesuchten Domänencontrollern täglich ein vollständiges Backup des Systemstatus (inkl. Active Directory) läuft. Dies sollte dann mindestens auf den Domänencontrollern laufen, die eine FSMO-Rolle beherbergen. Zum anderen sollte man darüber nachdenken, ob man nicht die „tombstone lifetime“ erhöht, zumal ja Microsoft dies auch mit Service Pack 1 implementiert hat. Es ist jedoch so, dass bei weitem die meisten Implementierungen des Active Directory nicht auf einem ersten Domänencontroller beruhen, der mit SP 1 aufgesetzt wurde. Eine Aktualisierung des Wertes auf 180 Tage - dem neuen Standard - bietet sich dabei auch tatsächlich an. Natürlich wird dadurch das Active Directory vom Volumen her größer, dies sollte aber weniger das Problem sein, denn der tägliche Replikationsverkehr vergrößert sich nicht. Nur bei einer Initialreplikation eines zusätzlichen Domänencontrollers entsteht ein größeres Volumen, wobei man dies auch noch umgehen kann. Siehe auch hierzu den weiteren Artikelverlauf.

Doch jetzt zurück zum Szenario. Die Organisationseinheit „Vertrieb“ wurde gelöscht (siehe Abbildung 9). Um diese Organisationseinheit nebst Inhalt wiederherstellen zu können und dies auch ohne den Rest zu beeinflussen, muss eine so genannte autoritative Wiederherstellung (authoritative restore) durchgeführt werden. Im dargestellten Szenario wird davon ausgegangen, dass die Sicherung mit Windows Bordmitteln gemacht wurde, also mit „Backup“ unter „Start – All Programs – Accessories – System Tools“. Hierfür ist dann insbesondere die Sicherung des „System State“ von Relevanz. Übrigens eine Sicherung des Active Directory in eine Datei auf diese Weise - spricht zeitgesteuert täglich - sollte bei der Planung des gesam-

```

C:\>tomstone.vbs
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.

Die Tombstone Lifetime wurde erfolgreich auf folgenden Wert gesetzt: 150

C:\>dsquery * "CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=domain,DC=com" -scope base -attr tombstonelifetime
tombstonelifetime
150
  
```

Abbildung 8: Setzen und kontrollieren der „tombstone lifetime“

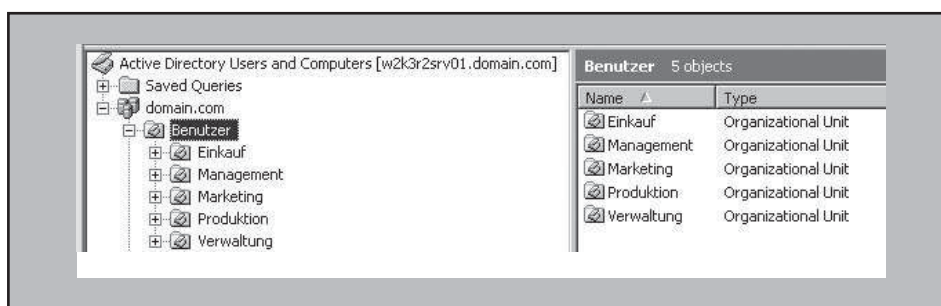


Abbildung 9: Organisationseinheit fälschlicherweise gelöscht

ten Backups eine Rolle spielen, da man in Ausnahmefällen dann unter anderem sehr schnell reagieren kann. Diese Sicherungsdatei sollte dann zusätzlich noch mit dem „normalen“ Backup gesichert werden. Ferner wird im Szenario auch das bereits vorgestellte Tool „NTDSUtil“ benötigt. Der erste Schritt, der dann zur Wiederher-

stellung durchgeführt werden muss, ist der Neustart des Domänencontrollers im so genannten „Directory Services Restore Mode“. Hierbei muss während des Startvorgangs im Fenster zur Auswahl des Betriebssystems „F8“ gedrückt werden, um ins „Windows Advanced Options Menu“ zu gelangen (siehe Abbildung 10). Durch

## REPORT

### Windows Server 2003 - Active Directory und IP-Management



Dieser Report beschreibt ausführlich alle Planungs- und Realisierungsaspekte einer Active-Directory-Infrastruktur basierend auf Windows Server 2003 und Active Directory Version 2. Es werden das vollständige Themenspektrum von der notwendigen IP-Infrastruktur hinsichtlich dynamischem DNS in Kombination mit DHCP sowie die Notwendigkeit von

WINS, die logische und physikalische Planung des Active Directory bis hin zur Standardisierung der Clientwelt über Gruppenrichtlinien behandelt. Darüber hinaus werden mögliche Migrationswege in die neue Welt beschrieben und bewertet. Abschließend erfolgt dann eine Betrachtung der Möglichkeiten zur Konsolidierung und zur Kopplung verschiedenster Verzeichnisdienste.

Autoren: Dipl.-Geol. Martin Gödde, Markus Holländer, Dipl.-Ing. Lars Kuhl, Frank Neunzig, Dipl.-Inform. Michael van Laak, Alexander Zarenko  
Preis: € 398,- zzgl. MwSt.



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

Troubleshooting Windows Server 2003 Active Directory - oft eine komplexe Sache!

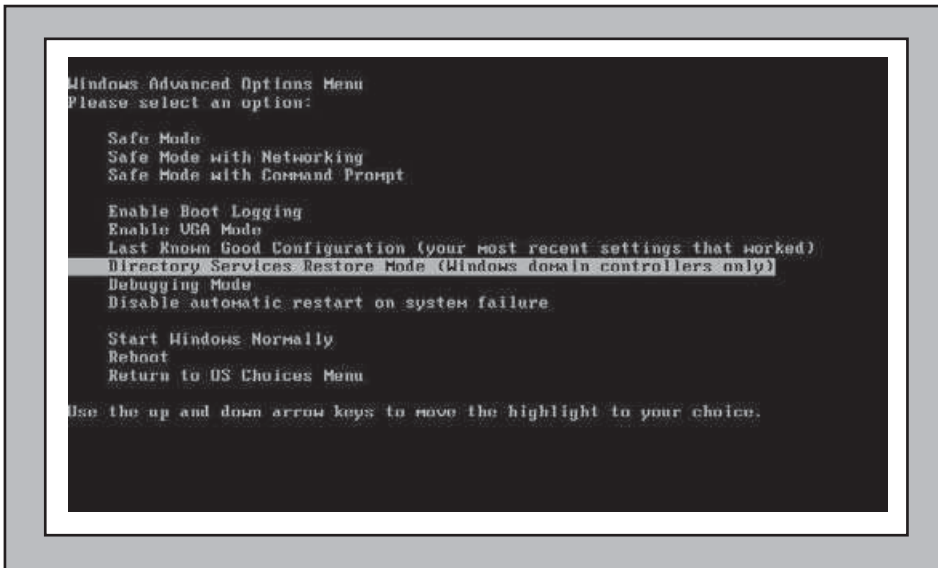


Abbildung 10: „Windows Advanced Options Menu“ während des Bootvorgangs

Auswahl von „Directory Services Restore Mode (Windows domain controllers only)“ erwirkt man dann den Bootvorgang im gewählten Modus. Im nächsten Menü muss man dann noch das zu startende Betriebssystem auswählen, in der Regel steht dort jedoch nur ein Auswahlpunkt zur Verfügung (Windows Server 2003[, Enterprise]). Im Anschluss erhält man noch den Hinweis, dass Windows sich im „safe mode“ befindet. Nicht zu vergessen ist, dass man sich während des Prozesses nochmals authentifizieren muss und dies mit dem Kennwort, welches während des DCPromo-Prozesses, für das Backup- bzw. Restore des Active Directory festgelegt wurde (siehe auch Abbildung 16: Directory Services Restore Mode Administrator Password). Dies könnte in Einzelfällen auch zu Problemen führen, falls man das Kennwort nicht parat hat oder ggf. schlimmer sogar vergessen und nicht hinterlegt hat.

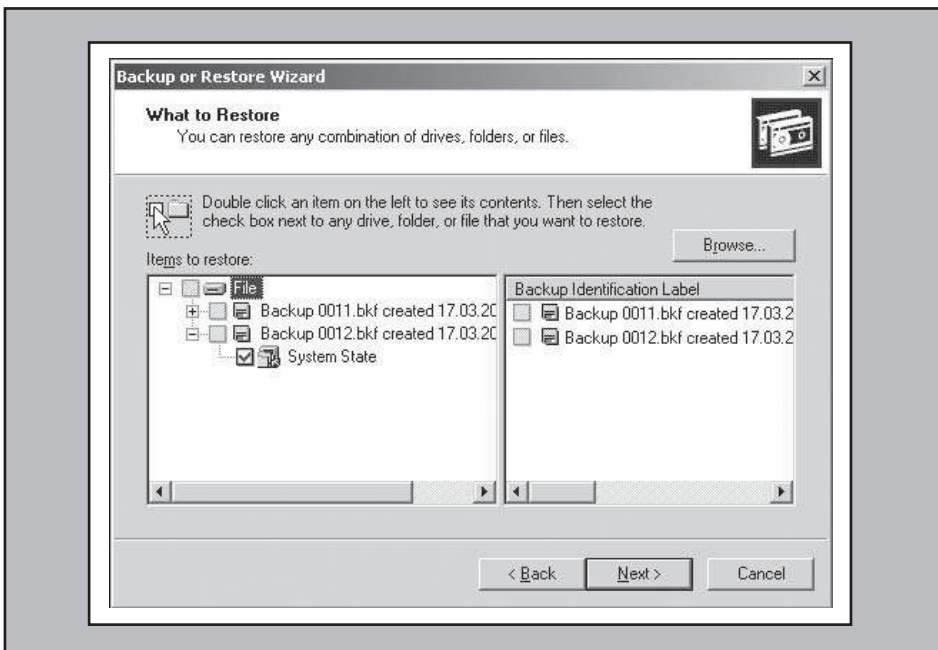


Abbildung 11: Wiederherstellung des System State

Nachdem der Domänenkontroller im gewählten „Restore Mode“ gestartet wurde, startet man das Backup-Tool. Man kann dann auch den Assistenten nutzen. Im Willkommensbildschirm wählt man „Next“, um dann im nächsten Fenster „Restore files and settings“ mit „Next“ zu bestätigen. Im Fenster „What to Restore“ wählt man dann den „System State“ der entsprechend zu verwendenden Sicherung (siehe Abbildung 11). Im nächsten Fenster wählt man dann noch „Advanced“ aus. Hierüber gelangt man dann zu den erweiterten Optionen, wo zuerst definiert wird, dass man „Restore files to“ „Original Location“ auswählt und dann mit „Next“ fortfährt. Im nächsten Fenster bestätigt man „Leave existing files“ mit „Next“. Unter „Advanced Restore Options“ sollten dann die folgenden Checkboxes gewählt werden: „Restore security settings“, „Restore junction points, but not the folders and file data they reference“, „Preserve existing volume mount points“ und „When restoring replicated data sets, mark the resto-

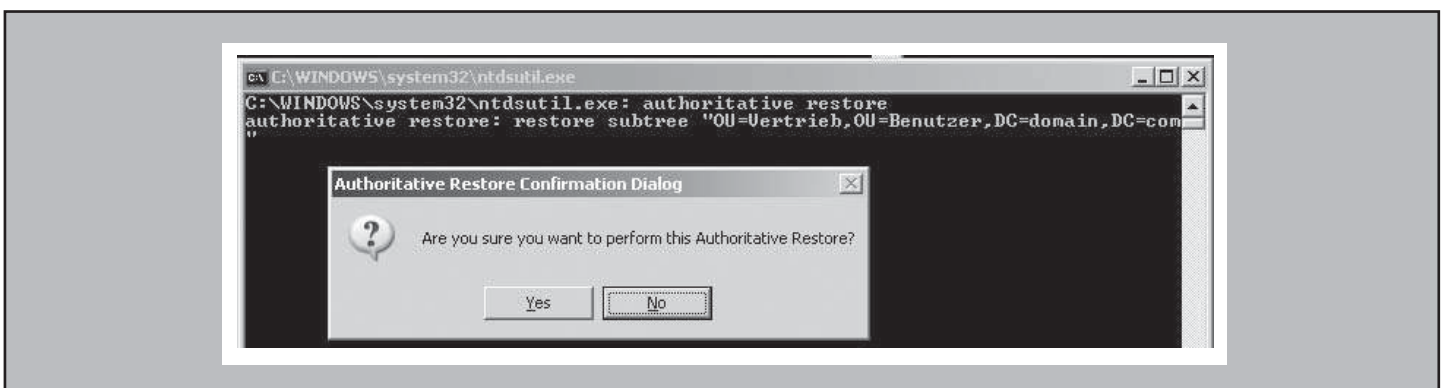


Abbildung 12: Nutzung von NTDSUtil für die autoritative Wiederherstellung

## Troubleshooting Windows Server 2003 Active Directory - oft eine komplexe Sache!

red data as the primary data for all replicas". Im Anschluss wird mit "Finish" der Wizard beendet und die Wiederherstellung gestartet.

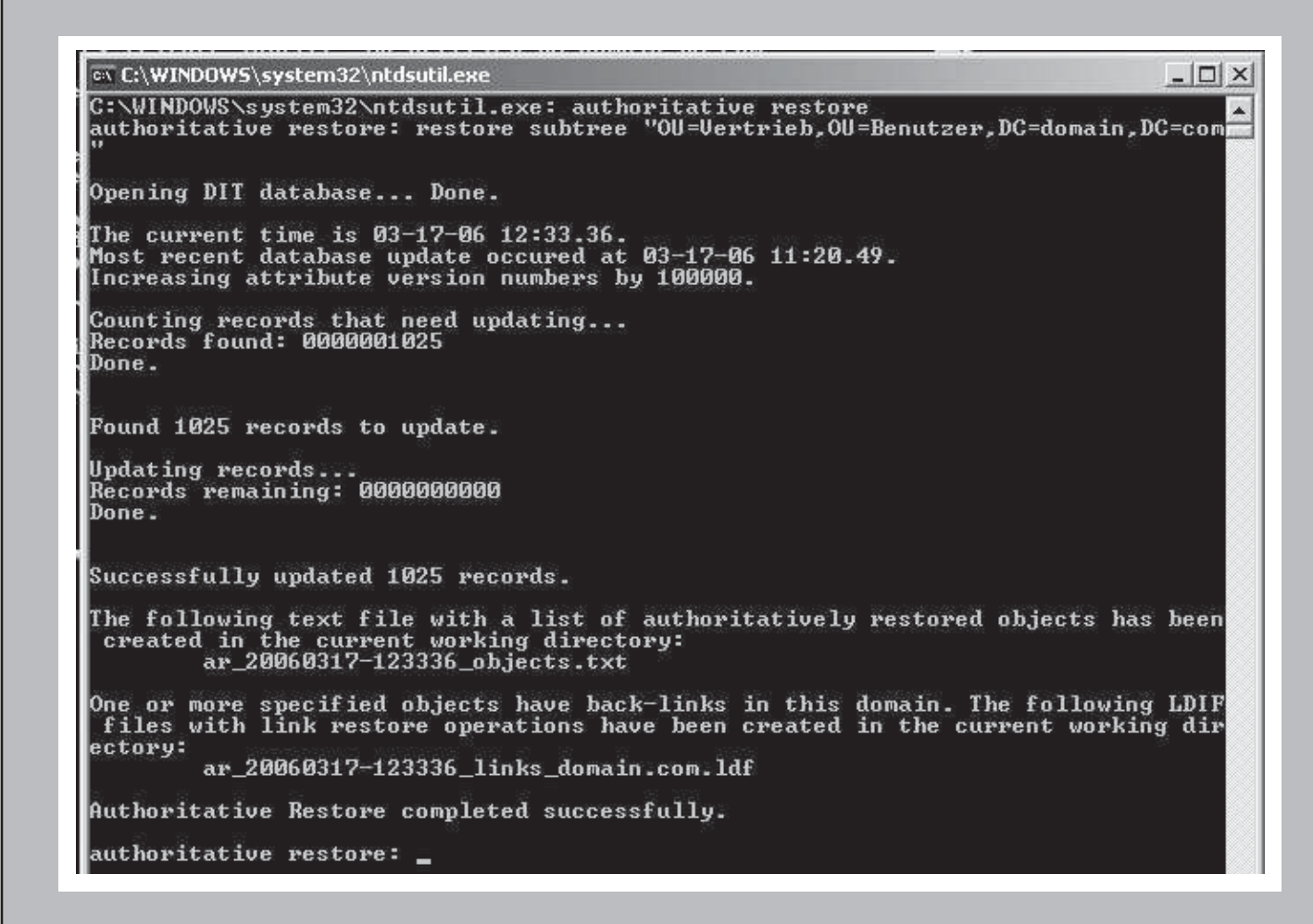
Nachdem der Wiederherstellungsprozess abgeschlossen ist, bestätigt man dies mit „Close“. Im anschließenden Fenster, ob der Domänencontroller wieder neu gestartet werden soll, wählt man dann „No“ aus, um im „Directory Restore“ Modus zu verweilen. Denn jetzt beginnt eigentlich erst der spannendere Teil. Unter „run“ (Ausführen) startet man unter Eingabe von „ntdsutil“ das gleichnamige Tool. Im Anschluss gibt man „authoritative restore“ ein, bestätigt mit „Enter“, um auch NTDSUtil im Wiederherstellungsmodus zu starten. Dann definiert man mit dem Befehl „restore subtree DistinguishedName“, was wiederhergestellt werden soll. „Restore subtree“ steht dann beispielsweise für die Wiederherstellung einer Organisationseinheit mit allen „child objects“, im nachgestellten Szenario also „restore subtree „OU=Vertrieb, OU=Benutzer,

DC=domain, DC=com““. Nach Bestätigung der Sicherheitsabfrage, erfolgt die Wiederherstellung der gewählten Organisationseinheit (siehe auch Abbildung 12 und Abbildung 13).

Wie in der Abbildung 13 zu ersehen ist, wurden 1.025 Records für die Wiederherstellung gefunden und auch erfolgreich wiederhergestellt. Ferner wurde definiert, dass die Wiederherstellung erfolgreich durchgeführt wurde. NTDSUtil unter Windows Server 2003 mit Service Pack 1 generiert aber auch noch 2 nützliche Dateien: 1. eine Textdatei mit den wiederhergestellten Objekten (siehe hierzu auch Anhang „ar\_20060317-123336\_objects.txt“, wo der erste Inhalt der Datei dargestellt wird) und 2. eine LDIF-Datei, die wiederhergestellte Objekte enthält, die so genannte „back links“ haben, die noch wiederherzustellen sind (siehe auch hierzu den Inhalt einer solchen Datei „ar\_20060317-123336\_links\_domain.com.ldf“). Kurz zur Erläuterung: Abhängig vom „Functional Level“, in dem sich die Ge-

samtstruktur befand, als die Gruppen erstellt wurden bzw. der Benutzer den Gruppen hinzugefügt wurde bzw. die Gruppe zuletzt aktualisiert wurden, kann es sein, dass für autoritative wiederhergestellte Objekte, die Gruppenzugehörigkeit nicht automatisch wiederhergestellt wird. Es ist nämlich so, dass mit dem Functional Level „Windows Server 2003 interim“ bzw. auch „Windows Server 2003“ die so genannte „linked-value-replication“ (LVR) implementiert wird. Wenn „LVR“ aktiv ist, dann werden die Mitgliederattribute separat repliziert, wobei wenn LVR nicht aktiv ist, die Mitgliederattribute als einzelner Wert repliziert werden. Insgesamt führt dies dazu, dass bei inaktiven LVR die Mitgliedschaft nicht wiederhergestellt wird. Mit der bereitgestellten LDIF-Datei kann dies jedoch automatisiert nachgeholt werden.

Nochmals kurz zurück zum dargestellten Szenario. Zum Verlassen von NTDSUtil gibt man noch zweimal „quit“ ein. Im Anschluss startet man den Domänencontroller neu. Dies gilt für Domänencontroller



```

C:\WINDOWS\system32\ntdsutil.exe
G:\WINDOWS\system32\ntdsutil.exe: authoritative restore
authoritative restore: restore subtree "OU=Vertrieb,OU=Benutzer,DC=domain,DC=com"
"
Opening DIT database... Done.
The current time is 03-17-06 12:33.36.
Most recent database update occurred at 03-17-06 11:20.49.
Increasing attribute version numbers by 100000.
Counting records that need updating...
Records found: 0000001025
Done.
Found 1025 records to update.
Updating records...
Records remaining: 0000000000
Done.
Successfully updated 1025 records.
The following text file with a list of authoritatively restored objects has been
  created in the current working directory:
    ar_20060317-123336_objects.txt
One or more specified objects have back-links in this domain. The following LDIF
  files with link restore operations have been created in the current working dir
  ectory:
    ar_20060317-123336_links_domain.com.ldf
Authoritative Restore completed successfully.
authoritative restore: _
  
```

Abbildung 13: Zusammenfassung von NTDSUtil für die autoritative Wiederherstellung

## Troubleshooting Windows Server 2003 Active Directory - oft eine komplexe Sache!

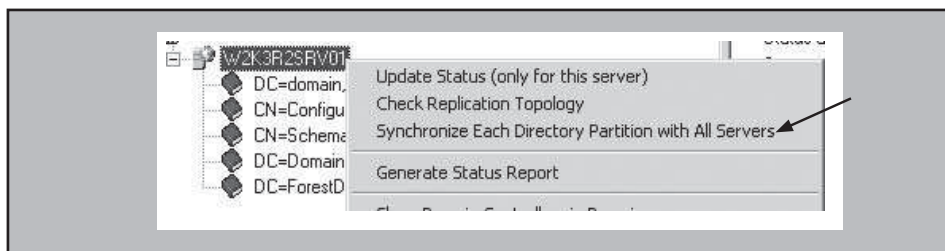


Abbildung 14: Kontextmenü eines Servers im Replication Monitor

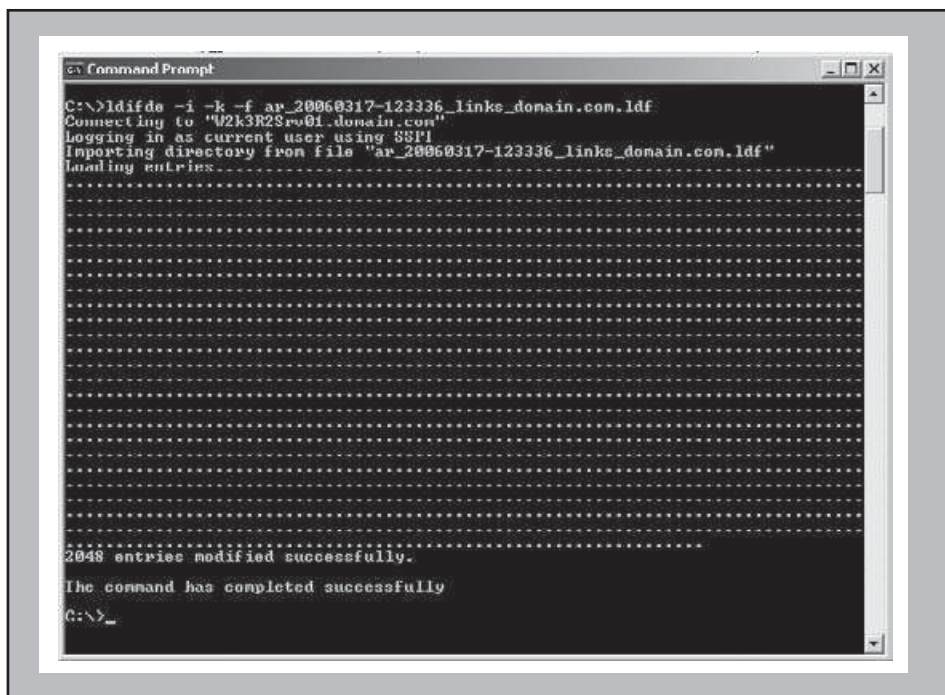


Abbildung 15: Ldifde zur Wiederherstellung der Gruppenzugehörigkeit

mit Service Pack 1. Für Domänenkontrollen ohne Service Pack 1 sind weitere Schritte erforderlich, die jedoch im Rahmen dieses Artikels nicht weiter behandelt werden.

Natürlich sollte man nach dem Neustart manuell eine vollständige Replikation erzwingen. Dies kann man zum einen mit dem „Replication Monitor“ in der GUI-Version machen (siehe Abbildung 14) oder per Kommandozeile mit den folgenden Befehl: „repadmin /synccall W2K3R2SRV01.domain.com /e /d /A /P /q“. (W2K3R2SRV1 ist der Server des nachgestellten Szenarios, wichtige Parameter sind: „/e“ für die Replikation auf allen Partnern aller Sites, /a für die Synchronisation aller Partitionen und /p für „Push“ der Infos).

Abschließend muss im dargestellten Szenario noch die Gruppenzugehörigkeit wiederhergestellt werden, wie bereits schon erläutert. Dazu benötigt man die erstellte Ldif-Datei. Im Verzeichnis, in der die

se Datei liegt, führt man folgenden Befehl aus: „ldifde -i -k -f ar\_20060317-123336\_links\_domain.com.ldf“. Wie in der Abbildung 15 zu sehen, sind 2.048 Objekte im dargestellten Szenario erfolgreich wiederhergestellt worden.

Nach diesem Schritt sind die „versehentlich“ gelöschte Organisationseinheit nebst Inhalt und weitere Abhängigkeiten wiederhergestellt. Auch dieses Szenario zeigt ganz deutlich, dass neben der Detailkenntnis (tombstone lifetime beispielsweise) auch wieder diverse „tiefergehende“ Tools (z.B. NTDSUtil, Replication Monitor) erforderlich sind.

### Dcpromo /adv

Im vorigen Szenario wurde kurz darauf hingewiesen, dass man für die Initialreplikation eines Domänenkontrollers auch anders vorgehen kann, als dies über das Netzwerk (ggf. standortübergreifend) zu replizieren. Hierzu verwendet man dann „dcpromo /adv“ (adv für advanced) in der Eingabeaufforderung, wenn man ei-

nen Domänenkontrollen - insbesondere einen zusätzlichen Domänenkontrollen für eine Domäne - integrieren möchte. Dadurch wird man dann in die Lage versetzt, die Daten für die Erstreplikation von einer Sicherung bzw. von einer Wiederherstellung zu verwenden. Hierzu sei angemerkt, dass die Sicherungsdatei auch vor Ort sein muss (ggf. sind mehrere hundert MBs oder mehr zu berücksichtigen) und dass vor der Ausführung von „dcpromo /adv“ eine Wiederherstellung an einem alternativen Ort („Alternate location“) erfolgen muss. An diesem Speicherort werden dann unter anderem auch die Informationen für das Active Directory hinterlegt. Bei der Auswahl des Verzeichnisses im „dcpromo“, wo die Daten wiederhergestellt wurden, ist nicht das Unterverzeichnis „Active Directory“ auszuwählen, sondern tatsächlich der alternative Speicherort. Die Informationen werden eigenständig aus dem Unterverzeichnis geholt. Nett ist auch noch die Nachfrage im „dcpromo“, ob man diesen Server auch zum „global catalog“ machen möchte. Natürlich kommt auch die Nachfrage für das „Directory Services Restore Mode Administrator Password“, welches ja das ein oder andere Mal dann doch benötigt wird, wie zuvor geschildertes Szenario zeigt.

Hat man dann sämtliche Informationen im „dcpromo“ eingegeben, dann startet auch die „Initialreplikation“ vom genannten Speicherort, was natürlich sehr schnell geht, da die Informationen alle lokal vorliegen und nur initialisiert werden müssen (siehe auch Abbildung 17).

### Resümee: Know-How erforderlich - Sie können es haben!

Insbesondere die zuvor ausführlich dargestellten beiden Szenarios haben gezeigt, dass das Troubleshooting im Bereich des Active Directory keine triviale Sache ist. Man benötigt detailliertes Wissen der Struktur und Konfiguration und auch für so manches Tool, was für einige Administratoren wohl nicht zum Standard zählen dürfte. Für alle, die obige Szenarios interessant finden, sei insbesondere das neue Troubleshooting Seminar zum Thema Windows Server 2003 Active Directory der ComConsult Akademie zu empfehlen. Diese und auch eine Reihe weiterer „Fälle“, die eigens für das Seminar aufbereitet werden bzw. wurden, werden dort detailliert erörtert. Dabei wird die Know-How-Grundlage aufgefrischt, das Thema mit Aufgaben gegengecheckt und auch so manches Szenario nachgestellt, so dass die Teilnehmer auch Hand anlegen müssen oder dürfen.

## Troubleshooting Windows Server 2003 Active Directory - oft eine komplexe Sache!

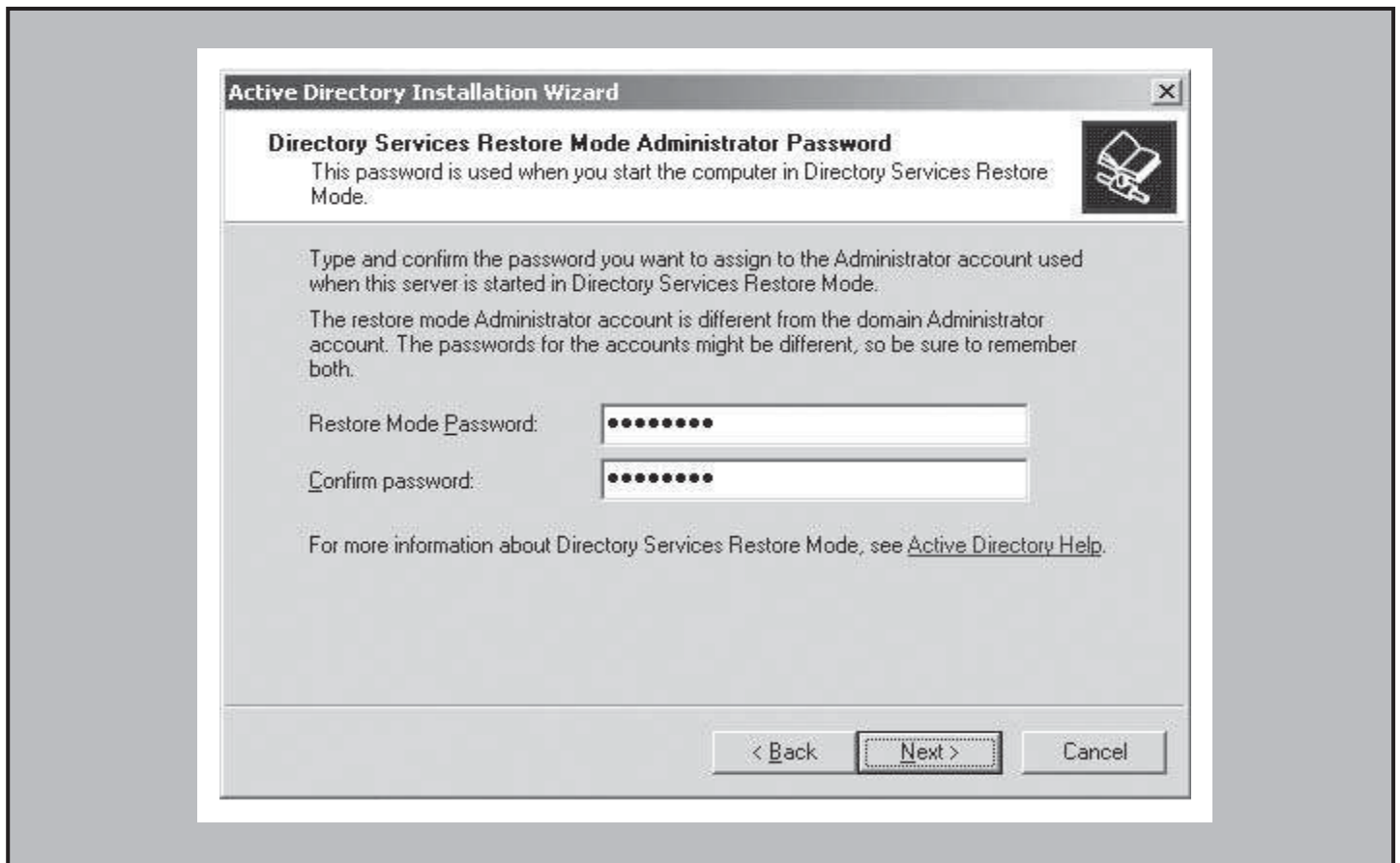


Abbildung 16: Directory Services Restore Mode Administrator Password

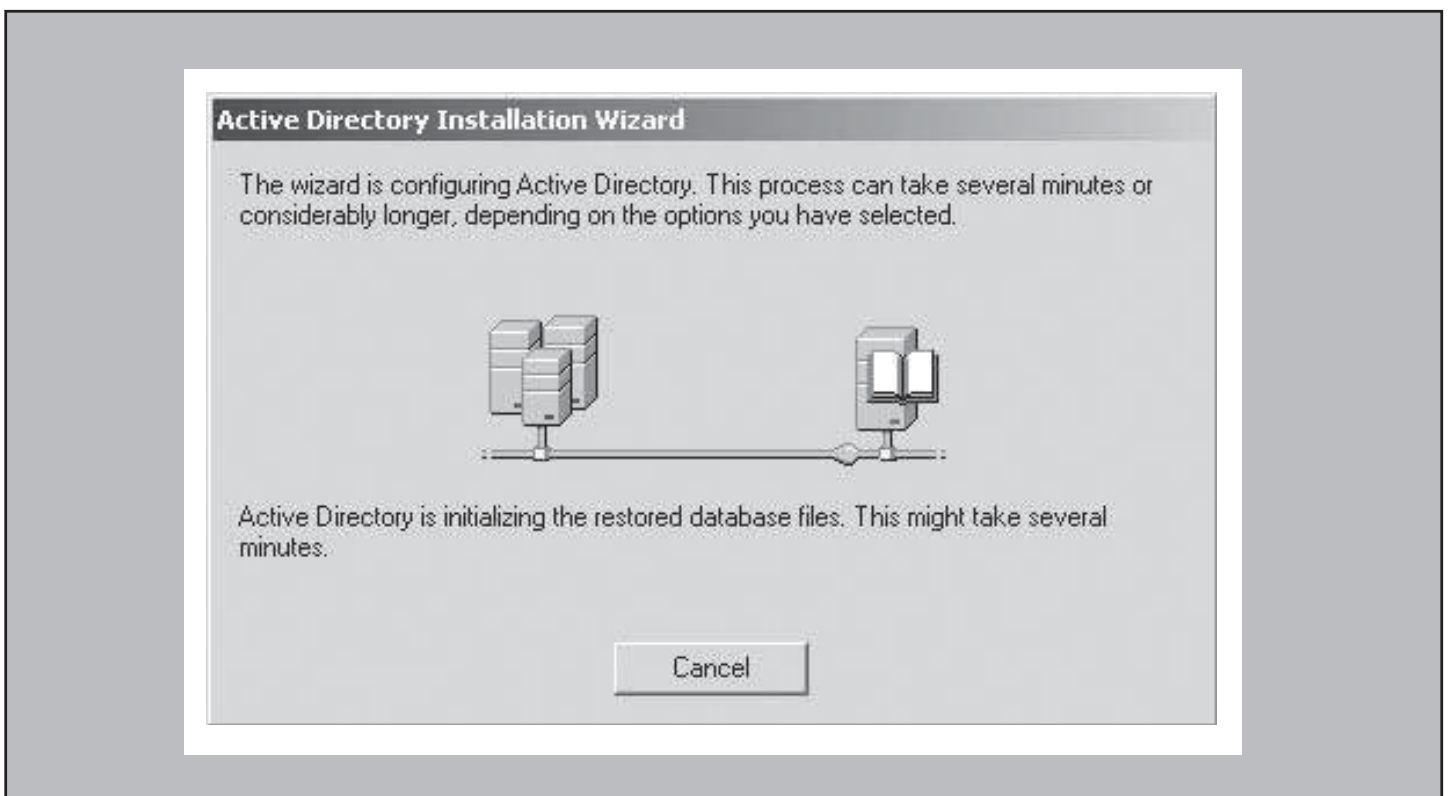


Abbildung 17: „dcpromo“: Initialisierung der wiederhergestellten Datenbank

---

 Troubleshooting Windows Server 2003 Active Directory - oft eine komplexe Sache!
 

---

**VBS Skript zur tombstone lifetime**

Folgendes Skript setzt die „tombstone lifetime“:

```
intTombstoneLifetime = 150

set objRootDSE = GetObject („LDAP://RootDSE“)
set objDSCont = GetObject („LDAP://cn=Directory Service,cn=Windows NT," & _
    „cn=Services," & objRootDSE.Get („configurationNamingContext") )
objDSCont.Put „tombstoneLifetime“, intTombstoneLifetime
objDSCont.SetInfo
WScript.Echo „Die Tombstone Lifetime wurde erfolgreich auf folgenden Wert gesetzt: „ & _
    intTombstoneLifetime
```

Es muss lediglich der grau hinterlegte Wert (hier 150) editiert werden.

Anhang 1

**ar\_20060317-123336\_objects.txt**

```
2801ee48-86b0-4e4a-b92a-d4c968193868;OU=Vertrieb,OU=Benutzer,DC=domain,DC=com
19636331-5e25-4174-91a2-3c6a01ac937d;CN=user004000,OU=Vertrieb,OU=Benutzer,DC=domain,DC=com
7c794287-4180-406a-846e-3d60d8219f23;CN=user004001,OU=Vertrieb,OU=Benutzer,DC=domain,DC=com
74d4cef5-7405-4b27-b9bc-99ffc00cdbfa;CN=user004002,OU=Vertrieb,OU=Benutzer,DC=domain,DC=com
0f3b2a93-d36b-49d0-94b1-8891fd159cfa;CN=user004003,OU=Vertrieb,OU=Benutzer,DC=domain,DC=com
bea2e0d7-4d60-4543-9b8c-06b10166d13e;CN=user004004,OU=Vertrieb,OU=Benutzer,DC=domain,DC=com
7fe7add8-6c6e-4b3c-8645-5e604e47f10d;CN=user004005,OU=Vertrieb,OU=Benutzer,DC=domain,DC=com
a9cf7e4c-bf3f-4e70-925a-94563fe04449;CN=user004006,OU=Vertrieb,OU=Benutzer,DC=domain,DC=com
a06218a6-a63b-4bd3-b8de-53c87dfce1bf;CN=user004007,OU=Vertrieb,OU=Benutzer,DC=domain,DC=com
7d5920c2-f2e4-4df5-9347-b8d2e0db479f;CN=user004008,OU=Vertrieb,OU=Benutzer,DC=domain,DC=com
6b191775-0f87-4d8b-9850-bd32aefa24b3;CN=user004009,OU=Vertrieb,OU=Benutzer,DC=domain,DC=com
18a2124a-45ff-45d5-a8c4-3e8457c32401;CN=user004010,OU=Vertrieb,OU=Benutzer,DC=domain,DC=com
cd7d8cc2-6931-4010-86ed-d6c5c7e7cb00;CN=user004011,OU=Vertrieb,OU=Benutzer,DC=domain,DC=com
55236ba6-ab3d-45f5-afdc-f2bd543d8576;CN=user004012,OU=Vertrieb,OU=Benutzer,DC=domain,DC=com
```

Anhang 2

**ar\_20060317-123336\_links\_domain.com.ldf**

```
dn: CN=Vertrieb,OU=Global,OU=Gruppen,DC=domain,DC=com
changetype: modify
delete: member
member: CN=user004000,OU=Vertrieb,OU=Benutzer,DC=domain,DC=com
-

dn: CN=Vertrieb,OU=Global,OU=Gruppen,DC=domain,DC=com
changetype: modify
add: member
member: CN=user004000,OU=Vertrieb,OU=Benutzer,DC=domain,DC=com
-

dn: CN=Vertrieb,OU=Global,OU=Gruppen,DC=domain,DC=com
changetype: modify
delete: member
member: CN=user004001,OU=Vertrieb,OU=Benutzer,DC=domain,DC=com
-

dn: CN=Vertrieb,OU=Global,OU=Gruppen,DC=domain,DC=com
changetype: modify
add: member
member: CN=user004001,OU=Vertrieb,OU=Benutzer,DC=domain,DC=com
-

dn: CN=Vertrieb,OU=Global,OU=Gruppen,DC=domain,DC=com
changetype: modify
delete: member
member: CN=user004002,OU=Vertrieb,OU=Benutzer,DC=domain,DC=com
```

Anhang 3

# Aktuelle Veranstaltungen

## **IP-Telefonie evaluieren, planen, betreiben, 24.04. - 26.04.06 Jolly Hotel in Köln**

Dieses 3-tägige Seminar evaluiert Technologien und Produkte gegenüber den in der Praxis bestehenden Anforderungen. Es vermittelt die technischen Grundlagen, beschreibt die Arbeitsweise wichtiger Produkte, analysiert typische Nutzungsformen und gibt eine Prognose für die Marktsituation und weitere Entwicklung. Die Situation etablierter Hersteller wie Alcatel, Avaya/Tenovis, Cisco, Nortel und Siemens inklusive des Leistungsumfangs ihrer Produkte wird bewertet.

Preis: € 1.690,- zzgl. MwSt.

## **Trouble Shooting für TCP/IP- und Windows-Umgebungen, 24.04. - 28.04.06 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.

## **Grundlagen des Trouble Shooting in Lokalen Netzwerken, 08.05. - 12.05.06 in Bad Neuenahr**

Dieses Seminar vermittelt, welche Werkzeuge die Basis für eine erfolgreiche Fehlersuche sind, wie man mit diesen Fehlersituationen analysiert und wie dabei methodisch vorgegangen wird, um in kürzester Zeit zu einem Ergebnis zu kommen.

Preis: € 2.490,- zzgl. MwSt.

## **Cisco Router erfolgreich einsetzen für Fortgeschrittene, 08.05. - 12.05.06 in Bonn**

Dieses 5-tägige Intensiv-Seminar wendet sich an Fortgeschrittene und hilft das Potenzial von Cisco Routern optimal auszuschöpfen sowie typische Fehler in der Konfiguration zu vermeiden. Es beinhaltet aktive Konfigurations-Übungen mit Cisco 2600 Routern in Kleinstgruppen. Schwerpunkt in diesem Seminar sind Redundanzkonzepte auf Layer 3.

Preis: € 2.350,- zzgl. MwSt.

## **Internetworking: optimales Netzwerk-Design mit Switching und Routing, 08.05. - 12.05.06 in Bonn**

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.

Preis: € 2.290,- zzgl. MwSt.

## **Quality of Service - QoS, 10.05. - 11.05.06 in Bonn**

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.

## **Projektmanagement I: Projekte erfolgreich leiten, organisieren und optimieren, 15.05. - 19.05.06 in Stuttgart**

In diesem 5-tägigen Intensiv-Kurs lernen Sie, ein Projekt erfolgreich zu leiten und organisieren. Es werden bewährte Wege aufgezeigt, wie Sie die Projektabwicklung im Alltag in Ihrem Unternehmen konkret optimieren.

Preis: € 2.290,- zzgl. MwSt.

## **Session Initiation Protocol SIP - Basis-Technologie der IP-Telefonie, 15.05. - 17.05.06 in Stuttgart**

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.

## **Troubleshooting Windows Server 2003 Active Directory, 15.05. - 17.05.06 in Aachen**

Das 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: € 1.690,- zzgl. MwSt.

## **Wireless LAN, 15.05. - 19.05.06 in Stuttgart**

Dieses 5-tägige Seminar erklärt die Arbeitsweise von WLANs und beschreibt typische Einsatzszenarien von der Ergänzung bestehender LANs bis hin zur kompletten WLAN-Infrastruktur. Die letzten beiden Tage sind optional buchbar und liefern vertiefte Kenntnisse zur Planung, Konfiguration und Betrieb von flächendeckenden sicheren WLAN und Hotspots, ergänzt durch praktische Beispiele und Demonstrationen.

Preis: € 2.290,- zzgl. MwSt.

## **TCP/IP und SNMP, 15.05. - 19.05.06 in Stuttgart**

Dieses 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.

Preis: € 2.290,- zzgl. MwSt.

CCNE

### ComConsult Certified Network Engineer

**Lokale Netze**

26.06. - 30.06.06 in Aachen  
23.10. - 27.10.06 in Neuss  
04.12. - 08.12.06 in Aachen

**Internetworking**

08.05. - 12.05.06 in Bonn  
11.09. - 15.09.06 in Aachen  
13.11. - 17.11.06 in Aachen

**TCP/IP und SNMP**

15.05. - 19.05.06 in Stuttgart  
25.09. - 29.09.06 in Köln  
27.11. - 01.12.06 in Berlin

**Ethernet Technologien - neuester Stand**

29.05. - 02.06.06 in Aachen  
25.09. - 29.09.06 in Aachen  
27.11. - 01.12.06 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**

08.05. - 12.05.06 in Bad Neuenahr  
04.09. - 08.09.06 in Aachen  
06.11. - 10.11.06 in Aachen

**Trouble Shooting in geswitchten Ethernet-Umgebungen**

19.06. - 23.06.06 in Aachen  
18.09. - 22.09.06 in Aachen  
13.11. - 17.11.06 in Aachen

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

24.04. - 28.04.06 in Aachen  
16.10. - 20.10.06 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**

15.05. - 19.05.06 in Stuttgart  
11.09. - 15.09.06 in Bonn

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

26.06. - 30.06.06 in Aachen  
23.10. - 27.10.06 in Aachen

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

19.06. - 21.06.06 in Aachen  
25.09. - 27.09.06 in Köln

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