Ulrich Schlüter

Integrationshandbuch Microsoft-Netzwerk

Galileo Computing

Auf einen Blick

Teil I

Teil II

Inhalt

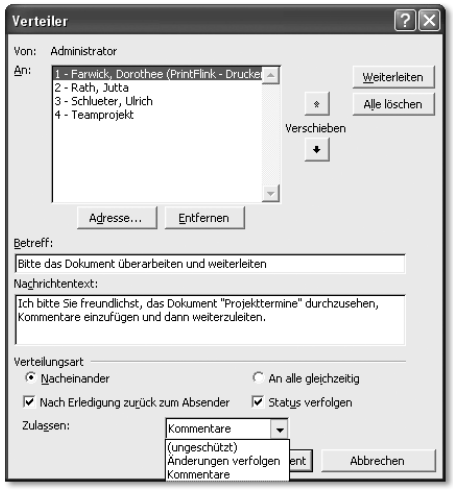
3.7.4 Senden eines Dokuments an eine Verteilerliste

Wenn Sie direkt aus einer Office-Anwendung wie Word den Befehl **Datei · Senden · Verteilerempfänger** wählen, so starten Sie damit einen Workflow: Sie suchen mehrere Empfänger aus, denen das Dokument nacheinander oder gleichzeitig zugesandt wird. Diese dürfen entweder direkte Änderungen am Original vornehmen oder nur Kommentare einfügen.

Wenn Sie die Option **Änderungen verfolgen** aktivieren, kann jeder weitere Empfänger in der angegebenen Reihenfolge die Änderungen der Vorgänger in der Kette der Zusendung als markierte Überarbeitungen verfolgen.

Wenn Sie die Option **Formulareingabe** aktivieren, können Sie ein Formular (z.B. einen Urlaubsantrag, einen Beschaffungsantrag oder eine Materialanforderung) versenden, das nur ausgefüllt, selbst aber nicht verändert werden darf.

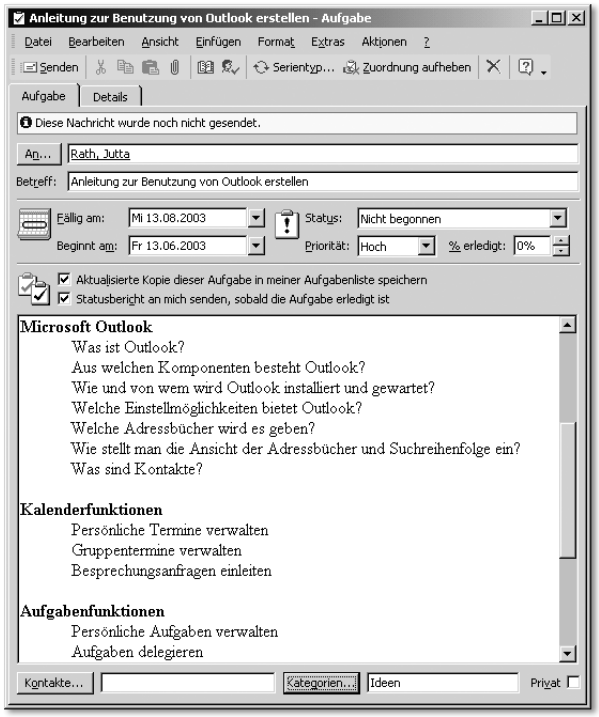
Wenn Sie die Option **Nach Erledigung zurück zum Absender** wählen, wird das Dokument automatisch an Sie zurückgeleitet, sobald der letzte Empfänger in der Kette es empfangen, bearbeitet und wieder geschlossen hat.



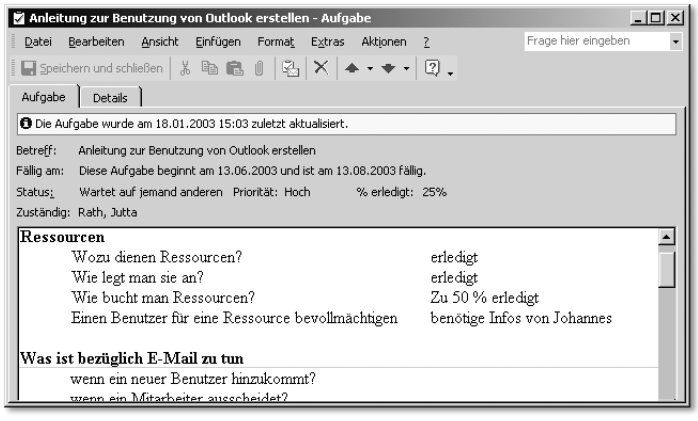
Die Option **Status verfolgen** bewirkt, dass Sie jedes Mal eine kurze E-Mail erhalten, sobald ein Empfänger in der Kette das Dokument an den nächsten Empfänger der Kette weiterleitet. Sie wissen also immer genau, bei welchem Mitarbeiter sich ein Vorgang zurzeit befindet.

3.7.5 Aufgaben zuweisen

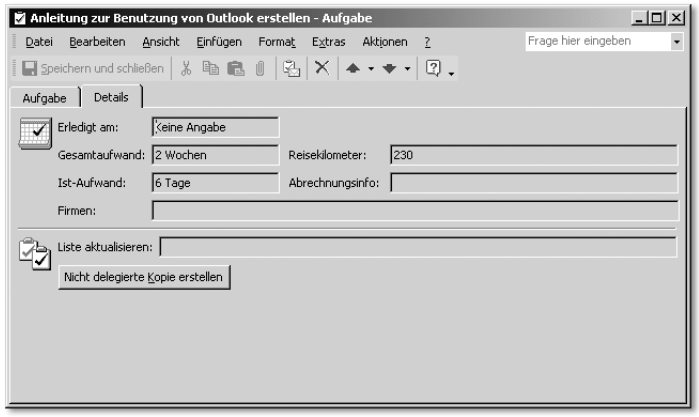
Ein Gruppenleiter kann eine neue Aufgabe erfassen und diese Aufgabe anschließend einem seiner Mitarbeiter zuweisen.



Der Mitarbeiter erhält die Aufgabenanfrage und kann die Aufgabe übernehmen oder auch begründet ablehnen. Wenn er die Aufgabe übernommen hat, kann er regelmäßig eingeben, wie viel Prozent der Aufgabe erledigt sind, ob die weitere Aufgabenerledigung von der Zuarbeit eines Dritten abhängig ist usw. Sobald er diesen Aufgabenstand wieder speichert, erhält der Gruppenleiter eine Information über den Stand der Aufgabenerledigung.



Füllt der mit der Aufgabenerledigung betreute Mitarbeiter die Registerkarte **Details** aus, so erhält der Gruppenleiter weitere Informationen über angefallenen Aufwand und Reisekilometer.

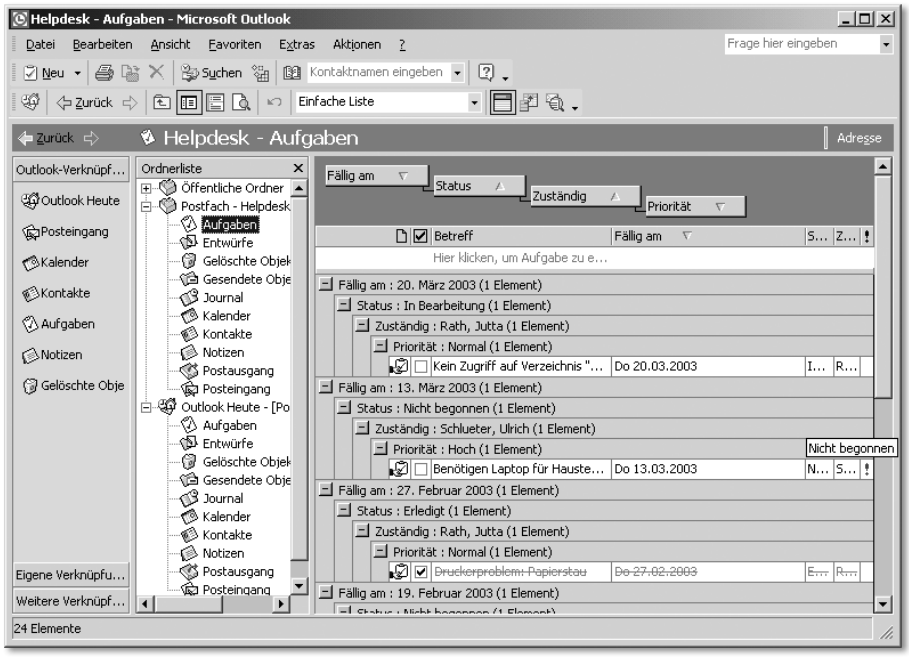


3.7.6 Einen Vertreter für ein Postfach bestimmen

Sobald Sie für einen Benutzer ein Exchange-Postfach angelegt haben, können Sie weitere Mitarbeiter oder Sicherheitsgruppen angeben, die dieses Postfach einsehen oder als Stellvertreter bearbeiten dürfen. Dazu wählen Sie im Snap-In **Active Diretory-Benutzer und -Computer** die Registerkarte **Exchange · Erweitert** dieser Kennung an und klicken auf die Schaltfläche **Postfachberechtigungen**. Wenn Sie zum Beispiel eine Benutzerkennung **Helpdesk** erstellen und für diese Kennung ein Postfach anlegen, so können Sie danach der Gruppe **IT-Abteilung** Zugriffsrechte für dieses Postfach erteilen.

Auf dieselbe Weise kann einer Sekretärin Zugriff auf das Postfach ihres Chefs erteilt werden. Ein Mitarbeiter der IT-Abteilung kann nun in Outlook das Postfach von **Helpdesk** hinzu laden, indem er unter **Extras · E-Mail-Konten · Vorhandene E-Mail-Konten anzeigen und bearbeiten** wählt, auf **Ändern** klickt, **Weitere Einstellungen** wählt und in der Registerkarte **Erweitert** unter **Zusätzliche Postfächer öffnen** das Postfach **Helpdesk** hinzufügt. Damit das Postfach jedoch hinzu geladen werden kann, müssen Sie sich zumindest einmal unter der Kennung **Helpdesk** anmelden und Outlook starten, denn erst dadurch wird das Postfach auf dem Exchange Server erzeugt.

Auf dieselbe Weise erzeugen Sie Kennungen und zugehörige Postfächer für Ressourcen wie Sitzungsräume, Projektoren, Beamer, Laptops oder Firmenfahrzeuge und schalten diese Postfächer anschließend zur Bearbeitung für diejenigen Mitarbeiter oder Mitarbeitergruppen frei, die die Ressourcen verwalten sollen. Eine Sekretärin kann auf diese Weise z.B. die Frei- und Gebuchtzeiten der Sitzungsräume mitverwalten. Ein Mitarbeiter der IT-Abteilung verwaltet die Ressourcen Beamer, Projektoren und Laptops mit.

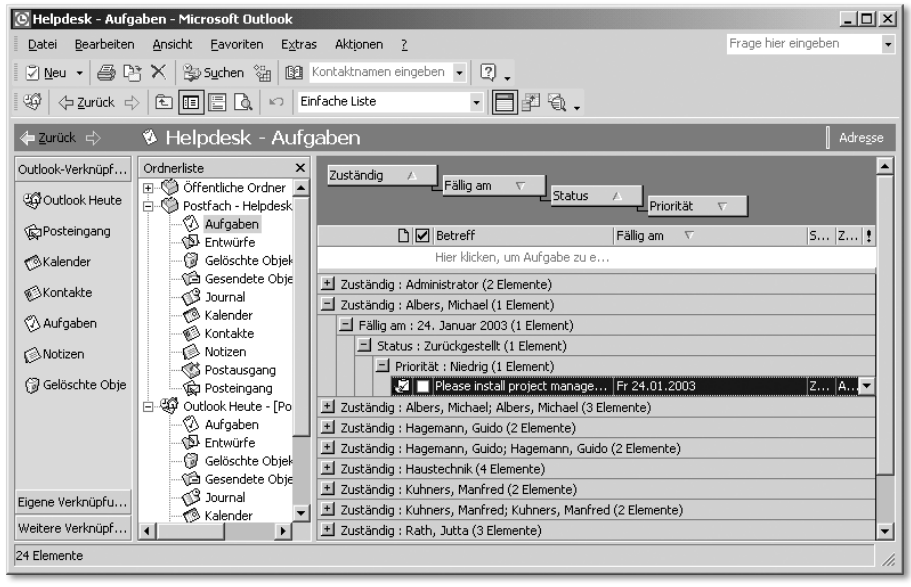


Ein Anwender kann nun eine Terminanfrage für ein Meeting im Sitzungsraum XYZ an die gewünschten Meeting-Teilnehmer verschicken und gleichzeitig den Sitzungsraum und einen benötigten Beamer für das Meeting buchen. Ebenso könnte er für das Meeting beim Kantinenchef Kaffee und Kuchen mitbuchen.

3.7.7 Eine kostenlose Helpdesk-Verwaltung

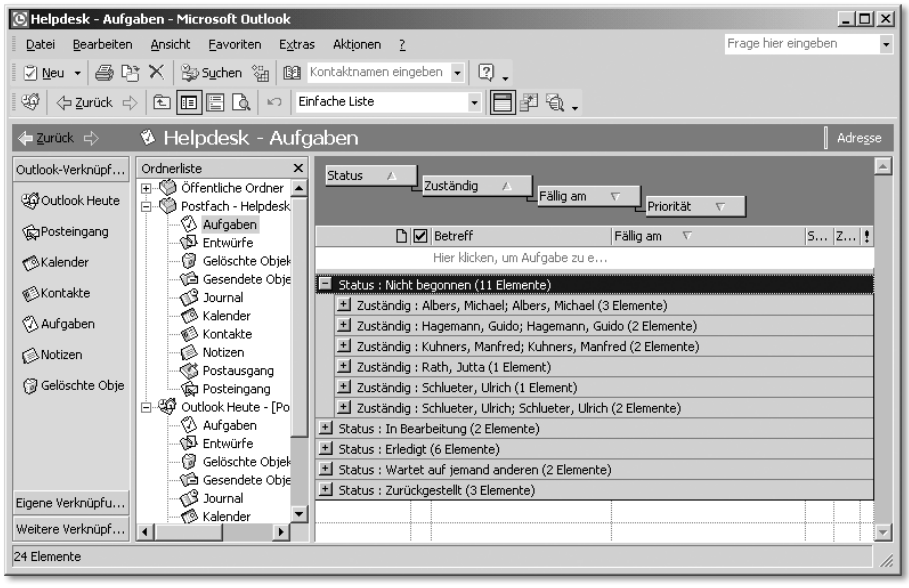
Die erzeugte und mit einem Exchange-Postfach versehene Kennung **Helpdesk** erfüllt jedoch noch andere Aufgaben. Sie wählen bestimmte Mitarbeiter der IT-Abteilung als postfachberechtigte Personen aus. Diese Mitarbeiter laden das Postfach der Kennung **Helpdesk** zu ihrem eigenen Postfach hinzu. Mitarbeiter des Unternehmens können nun Nachrichten an die Kennung **Helpdesk** schicken, in denen Sie ihre IT-Probleme nennen oder Aufgaben für die IT-Abteilung formulieren. Der Mitarbeiter der IT-Abteilung zieht die im Postfach **Helpdesk** eingehenden Nachrichten in den Container **Aufgaben** des Postfachs **Helpdesk** und weist die so aus der Nachricht erstellte neue Aufgabe einem Experten der IT-Abteilung zu. Dieser Experte erhält die Aufgabenanfrage und nimmt sie an. Dadurch landet diese Aufgabe als Kopie in seinem eigenen Aufgabencontainer. Sobald er dieser Aufgabe den Status **erledigt** zuweist, erhält die Kennung **Helpdesk** eine Rückmeldung. Auch im Aufgabencontainer von **Helpdesk** ist dann der Status dieser Aufgabe auf **erledigt** gestellt.

Im den nachfolgenden Abbildungen ist die Mitarbeiterin Jutta Rath berechtigt, das Postfach von **Helpdesk** zu öffnen, die Aufgaben den Mitarbeitern der IT-Abteilung zuzuweisen und den Grad der Aufgabenerledigung zu überwachen. Sie hat dazu im Container **Aufgaben** des Postfachs **Helpdesk** eine Ansicht erzeugt, die alle Aufgaben zuerst nach dem Fälligkeitstermin, danach nach dem Status der Erledigung, dann nach dem für die Aufgabenerledigung zuständigen Mitarbeiter und zuletzt nach der Priorität der Aufgaben gruppierend ordnet.



Auf diese Weise hat sie alle Aufgabentermine im Griff und kann schnell agieren, wenn eine Aufgabe mit hoher Priorität den Fertigstellungstermin überschritten hat. Wenn Frau Rath mit der Maus das Feld **Zuständig** nach oben zieht, ändert sich die Ansicht. Jetzt sind die an die Mitarbeiter verteilten Aufgaben nach der Zuständigkeit geordnet. Ruft morgens ein Kollege aus der IT-Abteilung an und meldet sich krank, so aktiviert Frau Rath diese Ansicht, um schnell entscheiden zu können, welche Aufgaben dieser Kollege gerade bearbeitet und ob wichtige Aufgaben des ausgefallenen Kollegen einem anderen Mitarbeiter zugewiesen werden müssen.

Wenn jedoch Frau Rath die Aufgaben nach dem Feld **Status** als erstem Gruppierungsfeld umordnet, sieht Sie auf einen Blick, welche Aufgaben erledigt sind.



Frau Rath könnte einen weiteren Container **erledigte Aufgaben** erstellen und alle Aufgaben, die den Status **erledigt** haben, in diesen Container verlagern und damit archivieren.

Schnell dürften Ihnen weitere Anwendungsmöglichkeiten dieses Beispiels einfallen. Sie können die Aktivitäten von Außendienstmitarbeitern, Technikern oder Projektmitarbeitern über Möglichkeiten der Aufgabendelegierung effizient koordinieren. Jeder Abteilungsleiter kann seine Mitarbeiter mit Outlook und Exchange steuern und muss dazu keine neue Anwendung erlernen. Wenn Sie die Mitarbeiter bei der Einführung von Exchange Server und Outlook ziel-

Neustart der Installation

Startet einen fehlgeschlagenen Versuch zur Installation eines Betriebssystems neu, wenn der Installationsvorgang vor seiner Beendigung fehlschlägt.

Verwaltung und Problembehandlung

Stellt Tools für die Verwaltung und Problembehandlung bei Clientcomputern bereit. Dazu gehören Virenscanner für den Arbeitsspeicher, Aktualisierungen des Systemflash-BIOS und Diagnosedienstprogramme für den Computer. Diese Tools werden von Drittanbietern bereitgestellt.

6.13 Der Groveler-Dienst und das Verzeichnis SIS Common Store

Der RIS-Dienst erfordert eine separate Partition, in die ein Abbild der CD des Client-Betriebssystems (Windows 2000 bzw. XP Professional) sowie später die Komplettabbilder eingespielt werden. Diese Partition muss mindestens 2 GByte groß sein, darf nicht mit der Systempartition identisch sein und sollte keine anderen Daten enthalten. Wenn Sie jedoch später mehrere Komplettabbilder für die verschiedenen HAL-Typen ablegen möchten, benötigen Sie eine größere Partition. Bei der Installation des Musterservers **S1** wurde eine Partition **F:** mit einer Größe von 6 GByte vorgeschlagen.

Der durch RIS als automatischer Dienst gestartete Groveler-Dienst, den Sie unter der Bezeichnung **Einzelinstanz-Speicherung (Groveler)** unter dem Menüpunkt **Verwaltung · Dienste** finden, erzeugt auf der RIS-Partition das Verzeichnis **SIS Common Store**. SIS steht für **Single Instance Store**. Immer dann, wenn der RIS-Server wenig ausgelastet ist, erhält der Groveler-Dienst vom Serverbetriebssystem eine höhere Priorität und sucht die RIS-Partition nach gleichnamigen Dateien mit derselben Version ab. Von diesen identischen Dateien legt er dann ein Duplikat im Verzeichnis **SIS Common Store** ab und ersetzt die Originaldateien durch Verweise auf dieses Duplikat. Dadurch werden bei mehreren Abbildern, die in die RIS-Partition eingespielt werden, folglich alle mehrfach vorkommenden identischen Dateien nur durch ein Duplikat an einer Stelle ersetzt und massiv Plattenplatz gespart.

Wenn die RIS-Partition jedoch gesichert wird, wird auf dem Sicherungsband der ursprüngliche Platz benötigt, den die mehrfach vorkommenden Dateien belegten. Berücksichtigen Sie diesen Umstand bei der Auslegung der Backup-Hardware für den RIS-Server.

6.13.1 Der Groveler-Dienst spart Plattenplatz

Der Groveler-Dienst verringert den Platzbedarf der gespeicherten Daten. Da Installations-Abbilder zu etwa 90% die gleichen Dateien enthalten, lässt sich hier ein sehr hoher Anteil an Daten durch den Austausch von Originaldateien durch Verweise auf deren Speicherort reduzieren. Dadurch ist es möglich, mit relativ wenig Speicherplatz eine große Menge an verschiedenen Abbildern auf dem Server anzubieten. Der Groveler-Dienst läuft im Hintergrund mit geringer Priorität. Dadurch wird verhindert, dass zu viel Leistung des Servers in die Indizierung und den Austausch der Dateien durch Verweise investiert wird. Der Dienst arbeitet »intelligent« mit der Auslastung der CPU, sogar wenn der Server im Leerlauf ist. Das heißt, der Dienst steigert über die ersten Betriebsstunden langsam seine Last, um sicherzugehen, dass er keine anderen Systeme auf dem Server davon abhält, ihre Aufgaben zu erledigen. Wenn allerdings der verfügbare Speicherplatz auf einer SIS-Partition unter eine festgelegte Grenze fällt, steigert der Dienst seine Intensität für den notwendigen Zeitraum, um freien Raum zu schaffen.

Um die Intensität des Groveler-Dienstes zu steigern, kann man den Groveler-Dienst in den Vordergrundmodus schalten. Dazu muss man über den Befehl **expand <CD-ROM>:\i386\grovctrl.ex_ <%systemroot%>\system32\grovctrl.exe** das Utility **grovctrl.exe** in das Verzeichnis **%systemroot%\System32** einfügen. Über den Befehl **grovctrl.exe f <Laufwerksbuchstabe>** wird der Dienst auf dem entsprechenden Laufwerk in den Vordergrundmodus geschaltet. Dadurch wird die Intensität erhöht, mit der der Groveler-Dienst die Daten indiziert und durch Analysepunkte ersetzt. Gleichzeitig steigt auch die Prozessorlast dieses Prozesses an. Nachdem der Dienst seine Aufgabe erledigt hat, kehrt er automatisch wieder in den Hintergrundmodus zurück.

Ich selbst habe, als ich über die Funktionsweise des Groveler-Dienstes noch nichts wusste, den Hinweis nicht befolgt, für RIS eine separate Partition zu nutzen. Ich benutzte die Partition, auf der auch mein Software-Archiv lag. Irgendwann später habe ich dann irgendwann den Server neu installiert. Nach der Neuinstallation des Servers konnte ich das merkwürdige Verzeichnis **SIS Common Store** nicht zuordnen, das aus der vorherigenInstallation noch immer vorhanden war. Ich löschte es. Als ich versuchte, Software aus dem Software-Archiv zu installieren, stellte ich fest, dass viele exe-Dateien im Software-Archiv nicht mehr funktionierten und offensichtlich ersetzt oder zerstört worden waren. Zuerst vermutete ich, dass ein Virus zugeschlagen hatte. Als ich später las, was der Groveler-Dienst mit doppelten Dateien macht, ahnte ich die wirkliche Ursache für den Verlust meiner exe-Dateien. Sie waren durch SIS-Linkdateien ersetzt worden, und die Originale waren unter anderen Namen in

das Verzeichnis **SIS Common Store** verschoben worden. Dieses Verzeichnis hatte ich aber gelöscht … Hoffentlich ist mein Missgeschick eine Warnung für Sie!

6.14 Backup und Restore der RIS-Partition

Bei der Sicherung der RIS-Partition muss die eingesetzte Backup-Lösung die Funktionalität der Analysepunkte (Reparse Points) unterstützen, die der SIS-Dienst aus identischen Dateien erzeugt. Anderenfalls gehen diese Informationen verloren. Das Windows Server eigene Sicherungsprogramm **ntbackup.exe** ist in der Lage, diese Informationen zu verarbeiten. Durch die Bereitstellung der Datei **SISbkup.dll** wird die Verwendung der Analysepunkte ermöglicht. Dadurch können auch mehrfach vorhandene Dateien nur ein einziges Mal gesichert und sämtliche Verweise erhalten werden. Sollte eine andere Sicherungssoftware eingesetzt werden, ist der Hersteller zu diesem Punkt zu befragen. Wenn die Software in der Lage ist, mit Analysepunkten umzugehen, aber nicht auf die Datei **SISbkup.dll** zurückgreift, kann eine SIS-Partition gesichert werden. Allerdings wird dann jede Datei, die mehrfach vorhanden ist, auch mehrfach gesichert. Um die Platz sparenden Funktionen auch auf dem Sicherungsband zu nutzen, muss die Software die Datei **SISbkup.dll** aufrufen können.

Falls die Backup-Software diese Funktionalität nicht unterstützt, muss zur Rücksicherung der Partition der Platz bereitgehalten werden, den alle Daten physikalisch ohne SIS belegen würden, und nicht nur der Platz, den die Partition vor dem Backup physikalisch eingenommen hat.

Bevor ein Laufwerk, das mit SIS verwaltet wurde, zurückgesichert wird, muss der SIS-Dienst auch wieder auf dem Laufwerk und der Partition, auf dem die Rücksicherung durchgeführt werden soll, installiert werden, damit die Dateien hinterher auch wieder zur Verfügung stehen. Dies ist nur über die Installation der RIS-Dienste und der Auswahl des entsprechenden Laufwerks möglich. Dadurch wird SIS automatisch installiert.

6.15 Mehrere RIS-Server synchron halten

Wenn Sie Abbild-Unterverzeichnisse oder einzelne Dateien aus der RIS-Partition des RIS-Servers in ein Verzeichnis einer anderen Partition desselben Servers oder auf einen anderen Server kopieren, werden nicht die SIS-Linkdateien kopiert, sondern wieder die Originaldateien. Wenn Sie später mehrere RIS-Server an unterschiedlichen Standorten einsetzen wollen, können Sie somit ein auf dem RIS-Server **S1** erzeugtes neues Komplettabbild irgendwann nachts, wenn die WAN-Leitungen wenig ausgelastet sind, komplett auf die anderen

RIS-Server kopieren und somit alle RIS-Server bezüglich der verfügbaren Abbilder auf demselben Stand halten. Zum Kopieren können Sie z. B. das Tool **Robocopy** aus dem Windows Server Resource Kit verwenden.

Hierbei ist zu beachten, dass die RIS-Partition des Zielservers ausreichend groß sein muss. Da das Tool **Robocopy** zwar mit den Analysepunkten umgehen, diese aber nicht entsprechend auflösen kann, wird jede Datei so kopiert, als ob sie physikalisch vorhanden wäre. Dadurch vergrößert sich temporär der Platzbedarf der Dateien auf der Zielpartition erheblich. Nachdem das Kopieren der Daten stattgefunden hat, wird über den Groveler-Dienst die Datenmenge wieder deutlich reduziert. Dieser Vorgang kann beschleunigt werden, indem der Groveler-Dienst in den Vordergrund geholt wird und ihm eine hohe Priorität zugewiesen wird. Das entpackte Tool **grovctrl.exe** wird mit dem Befehl **grovctrl.exe f <Laufwerksbuchstabe>** aufgerufen. Dadurch wird die Intensität erhöht, mit der der Groveler-Dienst die Daten indiziert und durch Analysepunkte ersetzt. Gleichzeitig steigt auch die Prozessorlast dieses Prozesses an. Nachdem der Dienst seine Aufgabe erledigt hat, kehrt er automatisch wieder in den Hintergrundmodus zurück.

6.16 Weitere Informationen zu RIS, SYS und SYSPREP

Lesen Sie den Technet-Artikel »Technical Guide to Remote Installation Services«, um mehr über RIS und SIS zu erfahren. Lesen Sie den »Anhang B – Frequently Asked Questions« im Artikel »Step-by-Step Guide to Remote OS Installation«. Beachten Sie aber, dass diese Aussagen sich auf Windows 2000 Server und Windows 2000 Professional beziehen und nicht die Veränderungen einbeziehen, die sich bezüglich RIS durch Windows Server 2003 bzw. durch das Service Pack 3 zu Windows 2000 ergeben haben.

Weitere Quellen

194080 – HFX HotFixManager What Is It and How Do You Use It.mht

216937 – System Preparation Tool and Answer File Usage.mht

238552 – How to Install Hotfixes and Check Versions of Installed Hotfixes.mht

239004 – How to Allow Non-Root or Enterprise Administrators to Authorize RIS Servers in Active Directory.mht

240126 – Best Practices for Using Sysprep with NTFS Volumes.mht

246184 – How to Add Third-Party OEM Network Adapters to RIS Installations.mht

250380 – How to Remove Internet Connection Wizard and Outlook Express Icons from the Desktop in Windows 2000.mht

254078 – How to Add OEM Plug and Play Drivers to Windows Installations.mht

260375 – Limited Custom Settings in Setup Manager When Creating an Answer File for a Sysprep Installation.mht

263027 – How to Restore a Volume That Is Managed by Single Instance Storage.mht

277705 – PRB Answer File (Unattend_txt) File Has a Limitation of 256 Characters for OEMPnPDriversPath.mht

299840 – How to Use Sysprep with Windows Product Activation or Volume License Media to Deploy Windows XP.mht

304314 – How to Deploy Windows XP Images from Windows 2000 RIS Servers.doc

304314 – How to Deploy Windows XP Images from Windows 2000 RIS Servers.mht

304992 – How to Boot the Windows Preinstall Environment from a RIS Server by Using PXE-Enabled Clients.mht

308299 – Stop 0x21a Error Message Occurs If You Download a RIPrep Image.mht

308508 – Unable to Create Windows 2000 Server Image on RIS Server.doc

308508 – Unable to Create Windows 2000 Server Image on RIS Server.mht

308662 – How to Use Setup Manager to Create an Answer File in Windows 2000.mht

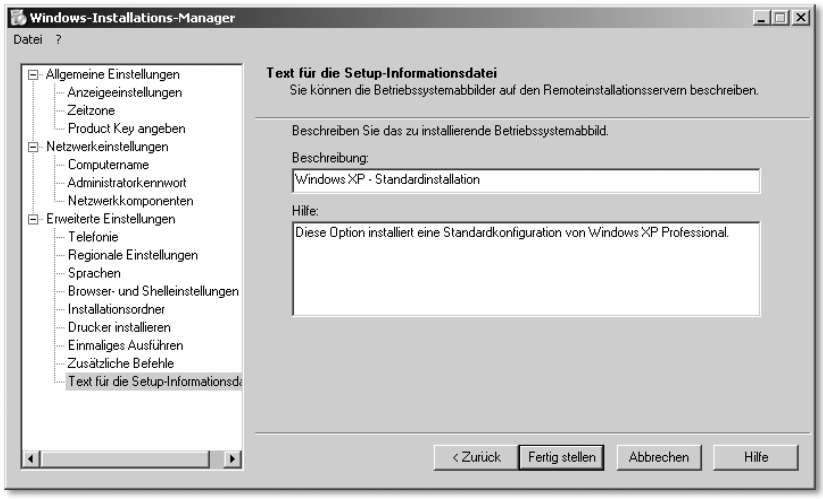
313069 – Update for the Riprep Tool.doc

314460 – System Preparation Tool and Answer File Usage.mht

315074 – Error Message: The Operating System Image You Selected Does Not Contain the Necessary Drivers for Your Network Adapter.mht

324722 – Versionsinformationen zu Windows XP Service Pack 1.mht

328096 – Setup Prompts You for the Windows XP SP1 CD or I386 Folder When You Try to Add a Windows Component.mht



Zuletzt werden Sie nach einem Speicherort für die neu generierte SIF-Datei gefragt.

7.3 Die Steuerdatei risndrd.sif manuell anpassen

Die mit dem Windows XP-Installations-Manager **setupmgr.exe** grundkonfigurierte Steuerdatei **risndrd.sif** zur automatischen Installation von Windows XP Professional von einem RIS-Server kann nun mit einem Editor überarbeitet werden. Selbstverständlich wird vorher eine Sicherungskopie angelegt. Übrigens können Sie viele der nachfolgend beschriebenen Änderungen an der **risndrd.sif** auch für die Steuerdatei **riprep.sif** übernehmen. Die **riprep.sif** steuert die automatische Installation eines Komplettabbildes des Betriebssystems Windows XP mit bereits installierten Anwendungen. Die Erstellung dieses RIPrep-Abbildes wird später ausführlich beschrieben.

Wenn Sie Hardwaretreiber von Drittanbietern verwenden müssen, die nicht von Microsoft digital signiert sind, können Sie im Abschnitt **[Unattended]** die Zeile **DriverSigningPolicy = Ignore** einfügen. Die Installation von Windows XP Professional würde sonst erwarten, dass die Installation eines nicht signierten Treibers bestätigt wird.

7.3.1 Auswahl der zu installierenden Windows XP-Komponenten

Sie sollten einen Abschnitt **[Components]** erstellen und dort die Installation derjenigen Windows XP-Komponenten deaktivieren, die nicht erwünscht sind, z.B. Spiele wie Freecell. Ebenso können Sie hier Komponenten aktivieren, die bei einer Standardinstallation nicht automatisch installiert werden. Die

Zeile **Freecell = Off** unterbindet z.B. die Installation des Spiels Freecell, die Zeile **LPDSVC = On** installiert automatisch die Unix-Druckdienste mit.

Aktualisierung von Stammzertifikaten	`Certsrv_client`
Faxdienste	`Fax`
Indexdienst	`indexsrv_system`
Internet Explorer	`IEAccess`
FrontPage 2000 Servererweiterungen	`fp_extensions`
FTP-Dienst	`iis_ftp`
SMTP- Dienst	`iis_smtp`
Snap-In Internet-Informationsdienste	`iis_inetmgr`
WWW-Dienst	`iis_www`
MSN Explorer	`Msnexplr`
Outlook Express	`OEAccess`
Druckdienste für Unix	`LPDSVC`
Windows Media Player	`WMPOCM`
Windows Messenger	`WMAccess`

Kategorie »Windows XP-Spiele«

Freecell	`freecell`
Hearts	`hearts`
Pinball	`pinball`
Spider	`spider`
Solitaire	`solitaire`
Internetspiele	`zonegames`
Minesweeper	`minesweeper`

Desktop-Hintergrund	`deskpaper`
Dokumentvorlagen	`templates`
Mauszeiger	`mousepoint`
Paint	`paint`
Rechner	`calc`
Zwischenablagenansicht	`charmap`
Audiorekorder	`rec`
Lautstärkeregelung	`vol`
Wordpad	`mswordpad`
Audio Schema	`media_utopia`
Audio Beispiele	`media_clips`
Hyperterminal	`hyperterm`
Wählhilfe	`dialer`

Der Abschnitt **[Components]** in der Steuerdatei **risndrd.sif** könnte folgenden Inhalt haben:

```
[Components]
; Spiele nicht installieren
Freecell = Off
Hearts = Off
Minesweeper = Off
Pinball = Off
Solitaire = Off
Spider = Off
Zonegames = Off
; Outlook Express nicht installieren
OEAccess = Off
; Automatisches Update von Windows-Komponenten nicht installie-
ren
AutoUpdate = Off
; Index Dienst nicht installieren
Indexsrv_system = Off
```

Ein wichtiger Tipp: Windows XP bietet bei der Installation und auch später in der Systemsteuerung unter Software keine Möglichkeit, ungewünschte Komponenten aus dem System zu entfernen. Wenn man in der Datei sysoc.inf im Verzeichnis C:\Windows\inf mit dem Editor Notepad.exe aber alle hide-Einträge entfernt, kann man unter Systemsteuerung – Software – Windows-Komponenten später wesentlich mehr Software-Komponenten sehen und auch entfernen. Die Datei sysoc.inf finden Sie aber auch im Verzeichnis RemoteInstall\setup\german\images\windowsxp\i386.

Erstellen Sie zuerst eine Sicherungskopie, bevor Sie die hide-Einträge entfernen. Folgende Komponenten sind in der sysoc.inf aufgelistet:

```
NtComponents = ntoc.dll,NtOcSetupProc,,4
WBEM = ocgen.dll,OcEntry,wbemoc.inf,hide,7
Display = desk.cpl,DisplayOcSetupProc,,7
Fax = fxsocm.dll,FaxOcmSetupProc,fxsocm.inf,,7
NetOC = netoc.dll,NetOcSetupProc,netoc.inf,,7
iis = iis.dll,OcEntry,iis.inf,,7
com = comsetup.dll,OcEntry,comnt5.inf,hide,7
dtc = msdtcstp.dll,OcEntry,dtcnt5.inf,hide,7
IndexSrv_System = setupqry.dll,IndexSrv,setupqry.inf,,7
TerminalServer = TsOc.dll, HydraOc, TsOc.inf,hide,2
msmq = msmqocm.dll,MsmqOcm,msmqocm.inf,,6
ims = imsinsnt.dll,OcEntry,ims.inf,,7
fp_extensions = fp40ext.dll,FrontPage4Extensions,fp40ext.inf,,7
AutoUpdate = ocgen.dll,OcEntry,au.inf,hide,7
msmsgs = msgrocm.dll,OcEntry,msmsgs.inf,hide,7
WMAccess = ocgen.dll,OcEntry,wmaccess.inf,,7
RootAutoUpdate = ocgen.dll,OcEntry,rootau.inf,,7
IEAccess = ocgen.dll,OcEntry,ieaccess.inf,,7
OEAccess = ocgen.dll,OcEntry,oeaccess.inf,,7
WMPOCM = ocgen.dll,OcEntry,wmpocm.inf,,7
Games = ocgen.dll,OcEntry,games.inf,,7
AccessUtil = ocgen.dll,OcEntry,accessor.inf,,7
CommApps = ocgen.dll,OcEntry,communic.inf,HIDE,7
MultiM = ocgen.dll,OcEntry,multimed.inf,HIDE,7
AccessOpt = ocgen.dll,OcEntry,optional.inf,HIDE,7
Pinball = ocgen.dll,OcEntry,pinball.inf,HIDE,7
MSWordPad = ocgen.dll,OcEntry,wordpad.inf,HIDE,7
ZoneGames = zoneoc.dll,ZoneSetupProc,igames.inf,,7
```

```
TabletPC = tabletoc.dll,TabletSetupProc,Tabletpc.inf,HIDE,7
msnexplr = ocmsn.dll,OcEntry,msnmsn.inf,,7
netfx = netfxocm.dll,UrtOcmProc,netfxocm.inf,hide,7
```

Bei einer Installation des Betriebssystems Windows XP Professional wird standardmäßig die erste Festplatte in der vollen Größe als Systempartition neu partitioniert und formatiert. Verantwortlich dafür sind die beiden Zeilen **Repartition = Yes** und **UseWholeDisk = Yes** im Abschnitt **[RemoteInstall]**. Für das Betriebssystem und die benötigten Standardanwendungen reicht jedoch in der Regel eine Partition **C:** mit 4 GByte. Leider gibt es keinen Parameter, mit dem man die gewünschte Größe der ersten Partition in der Steuerdatei **risndrd.sif** festlegen kann. Wenn Sie den Rest der Festplatte des Clients später für eine weitere Partition nutzen möchten, so können Sie folgenden Weg einschlagen:

Sie legen bereits vor der RIS-Installation des Betriebssystems auf dem Client eine entsprechend große Partition an, indem Sie mit einer Windows XP-CD starten und die Installation bis zu dem Punkt durchführen, an der eine Partition erstellt und mit NTFS formatiert wurde. Anschließend ändern Sie den Abschnitt **[RemoteInstall]** wie folgt ab:

```
[RemoteInstall]
Repartition = No
UseWholeDisk = No
```

Wenn Sie später ein Komplettabbild verteilen möchten und dieses RIPrep-Abbild von einem Quellcomputer erstellt wurde, bei dem die Systempartition z. B. 4 GByte groß war, so ändern Sie die zugehörige Steuerdatei **riprep.sif** wie folgt ab:

```
[RemoteInstall]
Repartition = YES
UseWholeDisk = NO
```

Das Komplettabbild soll ja auch auf neuen Computern installiert werden, auf denen noch keine Partition existiert oder die vom Hersteller mit einer Partitionierung geliefert wurden, welche nicht Ihren Vorstellungen entspricht. Folglich muss RIS die Festplatte neu partitionieren (Repartition = YES), aber nicht die komplette Festplatte für die erste Partition verwenden (UseWholeDiks = NO), sondern nur die im RIPrep-Image definierte Größe von 4 GByte.

Im Abschnitt **[data]** löschen Sie eine eventuell vorhandene Zeile **DisableAdminAccountOnDomainJoin = 1** oder deaktivieren Sie die Zeile durch ein Semikolon. Das Löschen entspricht dabei der Änderung des Wertes **1** in **0**. Ansonsten wird die lokale Administrator-Kennung deaktiviert:

```
[data]
; DisableAdminAccountOnDomainJoin = 1
```

Im Abschnitt **[Userdata]** tragen Sie die Kennung des Administrators und den Namen der Organisation ein. Unter Windows XP darf weder **Administrator** noch **Gast** eingetragen werden, wenn nach dem Namen des Benutzers gefragt wird, für den die Installation durchgeführt wird. Wenn Sie im Besitz eines Windows XP Professional-Organisationskeys sind, kann dieser über die Zeile **ProductID=...** eingetragen werden. Ohne diese Zeile muss später beim Ausrollen des Systems für jeden Computer ein Windows XP-Key eingetragen und aktiviert werden.


```
[UserData]
FullName = "SysAdmin"
OrgName = "Testfirma"
ComputerName = %MACHINENAME%
ProductID = xxxxx-xxxxx-xxxxx-xxxxx-xxxxx
```

Als Sie mit dem Windows XP-Installations-Manager **setupmgr.exe** die Steuerdatei **risndrd.sif** konfigurierten, konnten Sie ein Passwort für den lokalen Administrator eingeben und bestimmen, dass dieses Passwort in der Steuerdatei verschlüsselt eingetragen wird. Das verschlüsselte Passwort finden Sie jetzt im Abschnitt **[GuiUnattended]**:

```
[GuiUnattended]
OemSkipWelcome = 1
OemSkipRegional = 1
TimeZone = %TIMEZONE%
AdminPassword = db419622c8d7d104edd3ceb6b26416b1bdbed0fa6fb83b
EncryptedAdminPassword = Yes
```

Im Abschnitt **[Display]** geben Sie die einzustellende Standardauflösung und Bildwiederholfrequenz ein:

```
[Display]
ConfigureAtLogon = 0
BitsPerPel = 24
XResolution = 1024
YResolution = 768
VRefresh = 75
AutoConfirm = 1
```

Der Abschnitt **[OSChooser]** enthält die Beschreibung und den Hilfetext des Images. Diese Texte werden später im Abbild-Auswahlmenü des Client-Instal-

lationsassistenten angezeigt, wenn ein Helpdesk-Mitarbeiter einen neuen Computer mit dem Image bespielen möchte. Sie können die Texte hier ändern. Dies geht jedoch auch, indem Sie über das Snap-In **Active Directory-Benutzer und -Computer** die Eigenschaften des RIS-Servers öffnen, die Registerkarte **Remoteinstallation** wählen, **Erweiterte Einstellungen** anwählen und in der Registerkarte **Abbilder** die Eigenschaften des Abbildes bearbeiten:

```
[OSChooser]
Description = "Microsoft Windows XP Professional mit SP1"
Help = "Windows XP Professional mit SP1 wird automatisch instal-
liert, ohne dass der Benutzer zur Eingabe aufgefordert wird."
LaunchFile = "%INSTALLPATH%\%MACHINETYPE%\templates\star-
trom.com"
ImageType = Flat
Version = "5.1"
```

Beachten Sie: In der Steuerdatei **risndrd.sif** steht im Abschnitt **[OSChooser]** der Ausdruck **ImageType = Flat**. Wenn Sie später RIPrep-Abbilder, d.h. Komplettabbilder eines durchkonfigurierten Mustercomputers erstellen, steht in der zugehörigen Steuerdatei **riprep.sif** an dieser Stelle der Ausdruck **ImageType = SYSPREP** und der HAL-Typ des Quellcomputers in der Zeile **HalName =**:

Bei ACPI-APIC-Computern:

```
ImageType = SYSPREP
HalName = halaacpi.dll
```

Bei ACPI-PIC-Computern:

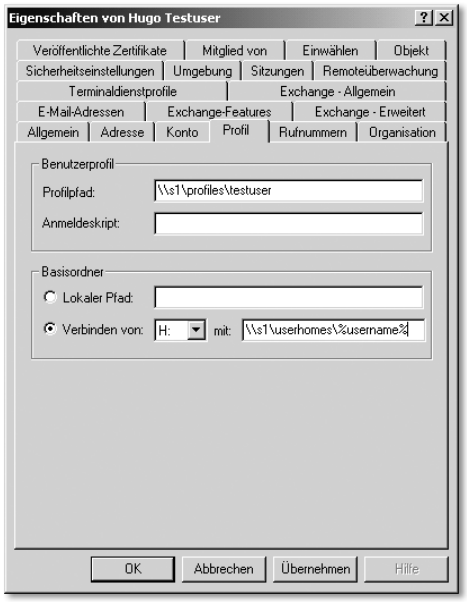
```
ImageType = SYSPREP
HalName = halacpi.dll
```

Bei Non-ACPI-APIC-Computern:

```
ImageType = SYSPREP
HalName = hal.dll
```

7.4 Zusätzliche OEM-Treiber installieren

Wenn Sie in die RIS-Installation des Betriebssystems zusätzliche Hardwaretreiber von Drittanbietern einbauen wollen, so ist das Verfahren im Artikel »254078 – How to Add OEM Plug and Play Drivers to Windows 2000« der Microsoft Technet beschrieben. Im Verzeichnis **RemoteInstall\Setup\German\Images\WindowsXP** erstellen Sie auf der gleichen Ebene, auf der sich



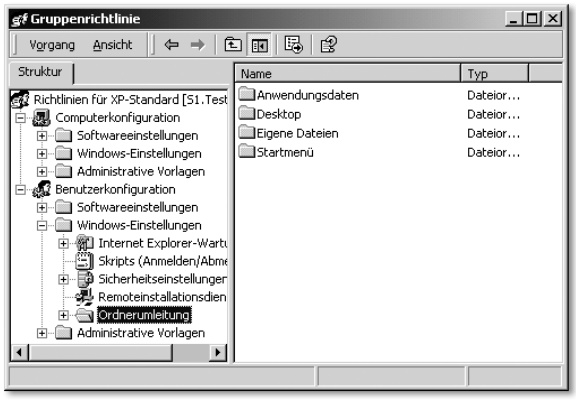
Auf das neu erstellte Verzeichnis haben die neue Kennung **Testuser** und die Gruppe **Administratoren** die Berechtigung **Vollzugriff**. Meldet sich der Benutzer **Testuser** an, so findet er im Microsoft Explorer unter dem Laufwerk **H:** sein Home Directory.

In den Microsoft Office XP-Anwendungen ist jedoch als Standardpfad für Dokumente immer noch der Ordner **Eigene Dateien** eingetragen. Der Ordner **Eigene Dateien** liegt jedoch unter **C:\Dokumente und Einstellungen\Testuser**. Da jedoch ein server-basiertes Benutzerprofil für die Kennung angelegt wurde, wird der Inhalt von **C:\Dokumente und Einstellungen\Testuser** bei jedem An- und Abmeldevorgang mit dem Serververzeichnis **\\s1\Profiles\testuser** synchronisiert. Dies führt einerseits zu ungewollter Netzlast, andererseits haben wir nicht ein Home Directory für den Benutzer angelegt, wenn seine Office-Dokumente anschließend an anderer Stelle gespeichert werden. Der Ordner **Eigene Dateien** muss also in das Home Directory umgeleitet werden.

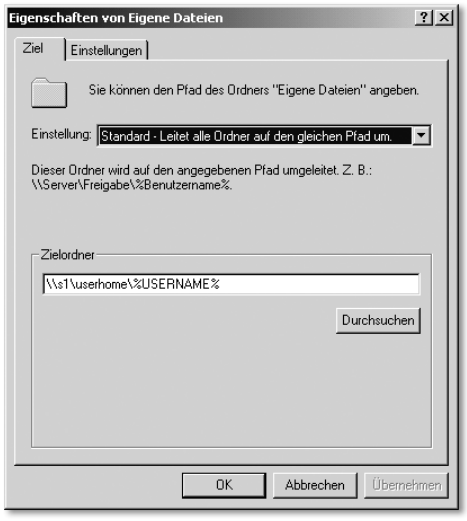
9.7 Eine Ordnerumleitung für das Verzeichnis »Eigene Dateien« einrichten

Im Kapitel zu den Windows XP-Vorlagedateien für Gruppenrichtlinien wird beschrieben, wie Sie die Vorlagedateien für Windows XP-Gruppenrichtlinien auf den Server einspielen und eine Organisationseinheit **Testfirma** und darunter die Organisationseinheit **Benutzer** anlegen. Lesen Sie bitte in diesem Kapi-

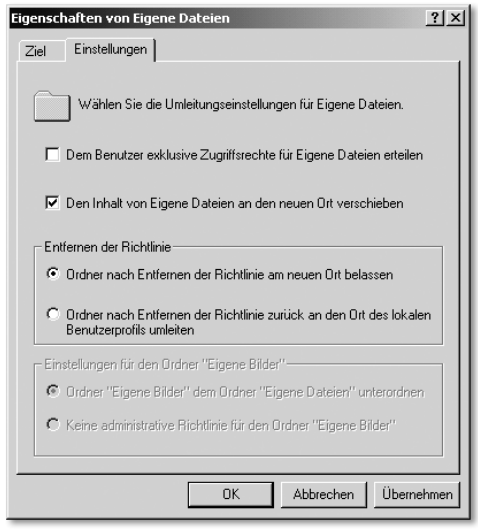
tel nach, wie Sie nun eine Gruppenrichtlinie namens »XP-Standardbenutzer« erstellen, die für alle Benutzer dieses Containers gilt. In dieser Gruppenrichtlinie finden Sie unter **Benutzerkonfiguration · Windows-Einstellungen** die Kategorie **Ordnerumleitung**.



Klicken Sie darin den Menüpunkt **Eigene Dateien** mit der rechten Maustaste an und wählen Sie **Eigenschaften**. Unter **Einstellung** können Sie die Option **Standard · Leitet alle Ordner auf den gleichen Pfad um** wählen und als Zielordner **\\s1\userhomes\%USERNAME%** eintragen.

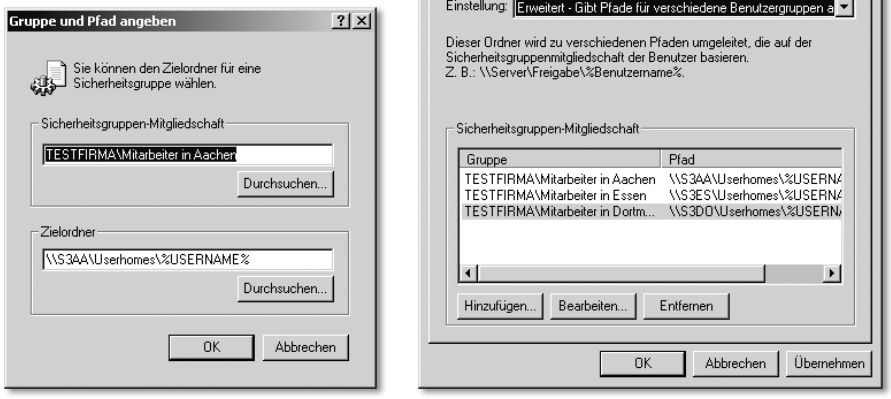


Danach kontrollieren Sie die Registerkarte **Einstellungen**. Deaktivieren Sie die Option **Dem Benutzer exklusive Zugriffsrechte für Eigene Dateien erteilen**, denn sonst können Administratoren anschließend wiederum nicht auf das Serververzeichnis zugreifen.



Melden Sie sich mit der Testkennung **Testuser** erneut an. Wenn Sie die Eigenschaften des Symbols **Eigene Dateien** auf dem Desktop starten, sehen Sie als Zielordner **\\s1\userhomes\testuser**, wobei der Anwender **Testuser** diese Vorgabe nicht ändern kann. In Word ist unter **Extras · Optionen** in der Registerkarte **Speicherort für Dateien** nun ebenso das Basisverzeichnis auf dem Server eingetragen, und auch das Standard-Dokumentenverzeichnis in Excel oder Powerpoint verweist auf das Serververzeichnis und nicht mehr auf die lokale Festplatte. Spätestens nach der Abmeldung ist der Inhalt des Ordners **Eigene Dateien** aus dem Verzeichnis **\\s1\Profiles\Testuser** in das Verzeichnis **\\s1\Userhomes\Testuser** verschoben worden, und auch der Unterordner **Eigene Bilder** liegt nun im Basisverzeichnis des Benutzers **Testuser**.

Die Richtlinie **Ordnerumleitung** bietet für die Umleitung des Ordners **Eigene Dateien** neben der Option **Standard · Leitet alle Ordner auf den gleichen Pfad um** die Option **Erweitert · Gibt Pfade für verschiedene Benutzergruppen an**. Wenn die Home Directories auf verschiedenen Servern liegen, so können Sie über diese Option den Ordner **Eigene Dateien** in Abhängigkeit von einer Gruppenmitgliedschaft verschieben. Gibt es z.B. die Standorte **Aachen**, **Essen** und **Dortmund** und an jedem dieser Standorte einen Dateiserver (z.B. die Dateiserver **S3AA** in Aachen, **S3ES** in Essen und **S3DO** in Dortmund), so erstellen Sie auf jedem Dateiserver eine Freigabe **Userhomes** und konfigurieren die Ordnerumleitung derart, dass für alle Mitglieder der Gruppe **Mitarbeiter in Aachen** der Ordner **Eigene Dateien** auf den Dateiserver in Aachen, für die Mitarbeiter in Essen und Dortmund der Ordner **Eigene Dateien** aber jeweils auf die lokalen Dateiserver in Essen und Dortmund umgeleitet werden.



Diese Richtlinie ist übrigens ein typisches Beispiel für eine Gruppenrichtlinie, die Sie nur einmal an zentraler Stelle definieren, zum Beispiel in einer speziellen Organisationseinheit **organisationsübergreifende Richtlinien**. In der Sub-OU **Benutzer** der Organisationseinheit **Dortmund** würden Sie dann eine Verknüpfung auf diese zentrale Gruppenrichtlinie erstellen. Wie das geht, lesen Sie später im Kapitel 12 »Die Gruppenrichtlinien von Windows XP einsetzen«.

Die letzte, mittels REM deaktivierte Zeile **if not exist %windir%\bestimmteDatei exit** zeigt Ihnen beispielhaft, wie Sie verhindern können, dass das Loginskript auf Computern gestartet wird, die nicht Ihrer Standard-Konfiguration entsprechen. Wenn sich z. B. alle Ihre Standardcomputer dadurch auszeichnen, dass es eine Datei **C:\WINDOWS\ABC.TXT** gibt, so würden Sie die Zeile entsprechend in **if not exist c:\windows\abc.txt exit** ändern und damit sicherstellen, dass das Skript niemals auf einem Computer abläuft, auf dem es diese Datei nicht gibt.

10.7 Für eine Gruppe von Anwendern ein Gruppenlaufwerk definieren

Um Netzlaufwerke zuzuweisen, kann man das Tool **ifmember.exe** aus dem Windows Server Resource Kit oder Kix32 verwenden. Die Syntax von **ifmember.exe** lautet beispielhaft:

```
ifmember.exe Domänenname\Gruppenname
if errorlevel 1 net use I: \\S1\Gruppenablage
```

Legen Sie zum Testen in der OU **Testfirma** die globalen Sicherheitsgruppen **Einkauf**, **Marketing**, **Produktion** und **Verkauf** an, und nehmen Sie die Kennung **Testuser** als Mitglied in die Gruppe **Verkauf** auf. Legen Sie auf dem Server **S1** ein Verzeichnis **Groups** an und geben Sie es unter dem Freigabenamen **Groups** frei. Erzeugen Sie unter dem Verzeichnis Groups einige Unterverzeichnisse wie **Einkauf**, **Verkauf**, **Marketing**, **Produktion**, und geben Sie vorerst nur das Unterverzeichnis **Verkauf** unter dem Freigabenamen **Verkauf** frei. Als Freigabeberechtigung wählen Sie **Vollzugriff** für die Gruppe **Jeder**.

Wählen Sie für das Verzeichnis **Verkauf** die Registerkarte **Sicherheitseinstellungen**. Entfernen Sie unten das Häkchen bei **Vererbbare übergeordnete Berechtigungen übernehmen**. Es öffnet sich ein Fenster **Sicherheitseinstellungen** mit dem Text **Sie haben die Übermittlung von vererbbaren Berechtigungen an diesem Objekt deaktiviert. Wie möchten Sie verfahren? Kopieren · Entfernen · Abbrechen**. Wählen Sie **Kopieren**. Wählen Sie jetzt die Gruppe **Benutzer** aus und entfernen Sie diese Gruppe. Wählen Sie **Hinzufügen** und geben Sie **Verkauf** ein. Geben Sie anschließend der Sicherheitsgruppe **Verkauf** das Recht **Ändern**.

Verfahren Sie ebenso mit den Sicherheitsrechten der drei Verzeichnisse **Einkauf**, **Marketing** und **Produktion**: Neben der Gruppe **Administratoren**, **ERSTELLER-BESITZER** und **SYSTEM** soll anschließend nur die gleichnamige Sicherheitsgruppe das Recht **Ändern** auf die jeweiligen Ordner besitzen.

Das Tool **ifmember.exe** liefert die Anzahl der Gruppen wieder, für die die Bedingung zutrifft. Gibt man den Befehl mit mehreren Gruppennamen hintereinander ein, so gibt der **Errorlevel** die Anzahl der Gruppen an, in denen der Anwender ein Mitglied ist. Die Abfrage **ifmember.exe gruppe1 gruppe2 gruppe3 gruppe4 gruppe5** liefert z.B. den Errorlevel 2, wenn der Anwender ein Mitglied von 2 der aufgezählten Gruppen ist.

Die folgenden Übungen werden mit der neuen Kennung **Mustermann** durchgeführt, für die keine Gruppenrichtlinien, keine Ordnerumleitung und kein server-gespeichertes Profil wirken, damit die Anmeldung schnell durchläuft und das Resultat der Änderungen von Übung zu Übung schnell überprüft werden kann. Legen Sie also eine neue OU **Testlogin** direkt in der Root der Domäne **Testfirma.de** an und erzeugen Sie dort ein neues Benutzerkonto namens **Martin Mustermann**. Für derartige Übungen, bei denen Sie sich ständig unter einer Testkennung an- und abmelden, sollten Sie in Ihrer Testdomäne auf ein Passwort verzichten.

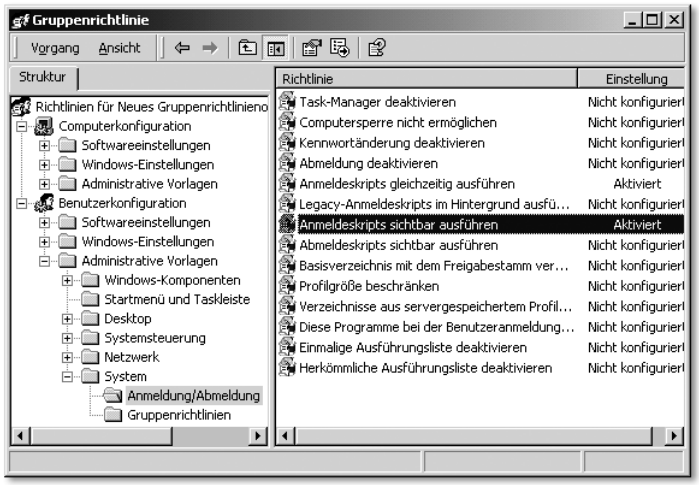
In der Registerkarte **Profil** geben Sie hinter **Anmeldeskript »ifmember1.cmd«** ein, wählen dann die Registerkarte **Mitglied von** und fügen die Kennung Mustermann in die Gruppe **Verkauf** ein.

Erzeugen Sie unter L: (= NETLOGON-Freigabe) die Batch-Routine **ifmember1.cmd**. Sie finden alle jetzt besprochenen Routinen auch auf dem Datenträger. Kopieren Sie das Tool **ifmember.exe** nach **L:\UTIL**. i**fmember1.cmd** hat folgenden Inhalt:

```
\\s1\netlogon\util\ifmember.exe testfirma\Verkauf
if errorlevel 1 net use g: \\s1\Verkauf
pause
```

Der letzte Befehl **pause** stoppt das Anmeldeskript, damit Sie sehen können, ob Fehler bei der Abarbeitung des Skripts auftauchen, und welche Meldungen ausgegeben werden.

Damit das Anmeldeskript nicht nur als kleine DOS-Box angezeigt wird, müssen Sie für die neue OU **Testlogin** eine Gruppenrichtlinie erzeugen, in der durch Aktivierung der Richtlinie **Anmeldeskripts gleichzeitig ausführen** erreicht wird, dass Sie sehen, was beim Ablauf des Loginskriptes geschieht.



Sie müssen sich eventuell zweimal hintereinander unter der Kennung Mustermann anmelden, damit die Richtlinie wirksam wird. Sobald die Anmeldung durchlaufen ist, starten Sie den Explorer und öffnen den Arbeitsplatz. Sie sollten folgendes Laufwerk sehen:**Verkauf auf »s1« (G:)**

Damit Sie sich nicht erneut ab- und anmelden müssen, geben Sie über **Start · Ausführen** den Befehl **\\s1\netlogon\ifmember1.cmd** ein. Bei der Abarbeitung der Befehlszeile **if errorlevel 1 net use g: \\s1\Verkauf** erscheint die Fehlermeldung **Systemfehler 85 aufgetreten**. Dieser Fehler beruht darauf, dass das Laufwerk **G:** bereits belegt ist und jetzt erneut belegt werden soll. Selbst wenn Sie sich als Mustermann abmelden und erneut anmelden, erscheint die Fehlermeldung, denn Windows merkt sich per Grundeinstellung die zuletzt verbundenen Laufwerke. Ändern Sie das Skript wie folgt ab:

```
net use g: /d
\\s1\netlogon\util\ifmember.exe testfirma\Verkauf
if errorlevel 1 net use g: \\s1\Verkauf
pause
```

Geben Sie über **Start · Ausführen** erneut den Befehl **\\s1\netlogon\ifmember1.cmd** ein. Das Laufwerk **G:** wird jetzt zuerst getrennt, bevor es erneut mit der Freigabe **\\s1\Verkauf** verbunden wird. Eine Alternative wäre, den Parameter **/persistent:no** hinter jeden net use-Befehl anzuhängen, damit sich Windows Laufwerkszuordnungen nicht merkt. Dennoch ist es sinnvoll, im Loginskript generell mittels des Befehls **net use Laufwerk: /del** sicherzustellen, dass der Laufwerksbuchstabe wirklich frei ist. Es könnte nämlich sein, dass ein Anwender selbst eine Laufwerkszuordnung gemacht hat, z.B. über den

Windows Explorer · Extras · Netzlaufwerk verbinden, und dabei das Häkchen vor der Option **Verbindung bei der Anmeldung wiederherstellen** nicht entfernt hat.

Testen Sie den Parameter **/persistent:no** aus, indem Sie in die **ifmember1.cmd** die Zeile **net use l: \\s1\netlogon /persistent:no** einfügen:

```
net use l: \\s1\netlogon /persistent:no
net use g: /d
\\s1\netlogon\util\ifmember.exe testfirma\Verkauf
if errorlevel 1 net use g: \\s1\Verkauf
pause
```

Setzen Sie über **Start · Ausführen** erneut den Befehl **\\s1\netlogon\ifmember1.cmd** ab. Unter **Arbeitsplatz** sollte jetzt das Laufwerk **L:** erscheinen. Deaktivieren Sie die erste Zeile, indem Sie sie durch ein vorangestelltes **rem** (Remark) auskommentieren: **rem net use l: \\s1\netlogon /persistent:no**

Melden Sie sich jetzt als **Mustermann** ab und wieder an. Laufwerk **L:** sollte dann nicht mehr vorhanden sein. Man kann übrigens generell über den Registry-Key **HKEY_CURRENT_USER\Software\ Microsoft\Windows NT\CurrentVersion\Network\Persistent Connections** und dort über die Zeichenfolge **SaveConnections** einstellen, ob sich Windows Netzwerk-Laufwerkszuordnungen merkt. Diese Zeichenfolge hat standardmäßig den Wert **yes** und sollte zu diesem Zweck auf **no** umgestellt werden. Nach der Umstellung können Sie eine reg-Datei durch Export des Schlüssels erstellen und dann über ein Loginskript bei allen Anwendern importieren. Auf der Buch-CD finden Sie die Datei **PersistentConnection.reg**, die diesen Key umstellt. Doch dazu später mehr. Sie können auch eine eigene Gruppenrichtlinien-Datei erzeugen, in der dieser Key umgestellt werden kann (siehe dazu die Datei **PersistentConnection.adm** auf der Buch-CD). Leider habe ich diese Gruppenrichtlinie in keiner der Microsoft Default-ADM-Dateien gefunden.

Vielleicht ist es in Ihrem Netzwerk jedoch gewollt, dass der Benutzer zumindest bestimmte Laufwerksbuchstaben selbst permanent mit Netzfreigaben verbinden kann. Sie sollten in diesem Fall eine Anzahl von Netzlaufwerken fest belegen (z.B. die Laufwerksbuchstaben **A:** bis **P:**) und dem Anwender mitteilen, welche Buchstaben für ihn verfügbar sind (die Buchstaben ab **O:**).

10.8 Exkurs zum Verständnis des Befehls »if errorlevel Zahl«

Der Errorlevel liefert beim Tool **ifmember.exe** die Anzahl der Gruppen wieder, in denen der Anwender ein Mitglied ist. Der Befehl **if errorlevel Zahl** oder auch seine Negation **if not errorlevel Zahl** kann jedoch generell dazu genutzt werden, den Erfolg oder Misserfolg von Befehlen abzufragen. Sie können sich den erzeugten Errorlevel einmal anzeigen lassen, indem Sie folgendes Loginskript dem Testuser zuweisen:

```
@echo off
ifmember.exe »Testfirma\Verkauf« »Testfirma\Einkauf«
echo %ERRORLEVEL%
pause
```

Machen Sie den Testuser zum Mitglied der Gruppen **Verkauf** und **Einkauf** und melden Sie sich unter der Kennung **Testuser** an. Bei der Abarbeitung des Loginskriptes erhalten Sie die Meldung **echo 2**, weil **Testuser** Mitglied von beiden Gruppen ist. Entfernen Sie die Kennung **Testuser** aus der Gruppe **Einkauf** und melden Sie sich erneut unter **Testuser** an. Sie erhalten die Meldung **echo 1**. Ändern Sie das Loginskript wie folgt ab:

```
@echo off
net use i: /d
ifmember.exe »Testfirma\Verkauf«
echo %ERRORLEVEL%
if errorlevel 1 echo %USERNAME% ist Mitglied von Verkauf!
echo %ERRORLEVEL%
if errorlevel 1 net use I: \\S1\Verkauf
echo %ERRORLEVEL%
pause
```

Melden Sie sich wieder als Testuser an. Sie erhalten folgende Meldungen:

```
1
testuser ist Mitglied von Verkauf!
Der Befehl wurde erfolgreich ausgeführt!
0
Drücken Sie eine beliebige Taste ...
```

Aus diesem Beispiel lernen Sie folgendes: Da **Testuser** Mitglied von **Verkauf** ist, ist der Errorlevel zuerst gleich 1. Der Befehl **echo %USERNAME% ist Mitglied von Verkauf!** wird zwar fehlerlos durchgeführt, verändert aber den Wert des Errorlevels nicht. Der nachfolgende Befehl **echo %ERRORLEVEL%** zeigt

einen unveränderten Errorlevel von 1 an. Der dann folgende Befehl **if errorlevel 1 net use I: \\s1\Verkauf** wird erfolgreich ausgeführt. Folglich ist danach der Wert des Errorlevels gleich 0. Mit der Abfrage des Errorlevels kann man also den Erfolg von Befehlen abfragen. Hätten Sie vergessen, das Verzeichnis **Verkauf** freizugeben, oder hätten Sie sich vertippt und statt **if errorlevel 1 net use I: \\s1\Verkauf** den Befehl **if errorlevel 1 net use I: \\s1\Verkoff** eingefügt, so würden Sie folgende Meldungen erhalten:

```
1
testuser ist Mitglied von Verkauf!
Systemfehler 53 aufgetreten.
Der Netzwerkpfad wurde nicht gefunden.
2
Drücken Sie eine beliebige Taste …
```


Sie können also mit der Abfrage des Errorlevels feststellen, ob Befehle erfolgreich abgearbeitet wurden. Wenn sie fehlerhaft abgearbeitet wurden, können Sie aufgrund des erzeugten Errorlevels alternative Schritte einleiten.

Im folgenden Beispiel führt der Befehl **net use I: \\S1\Verkoff** zu einem Errorlevel, der größer als 0 ist. Mittels der nachfolgenden echo-Befehle werden drei Meldungen auf dem Bildschirm erzeugt. Der Befehl **echo** mit angehängtem Punkt **echo.** erzeugt eine Leerzeile, damit die durch den pause-Befehl erzeugte Aufforderung **Drücken Sie eine beliebige Taste…** von diesen Meldungen optisch getrennt wird. Sobald der Anwender dann eine Taste drückt, wird das Loginskript mit dem Befehl **exit** an dieser Stelle beendet.

```
@echo off
net use I: /d
ifmember.exe »Testfirma\Verkauf«
if errorlevel 1 net use I: \\S1\Verkuff
if not errorlevel 0 goto OKAY
   echo Fehler in der Ausführung des Loginskriptes
   echo Melden Sie sich bei der Systemadministration!
   echo Die weitere Abarbeitung des Loginskriptes wird abgebro-
chen.
   echo.
   pause
   exit
:OKAY
echo Das Laufwerk I: wurde erfolgreich mit der Freigabe Verkauf
verbunden.
pause
```

In obigem Beispiel hätte der Befehl **if errorlevel 0 goto OKAY** übrigens nicht das gewünschte Resultat gebracht. Nimmt nämlich der Errorlevel z. B. den Wert **2** an, so hat er gleichzeitig auch alle Werte unterhalb von **2**, also den Wert **1** und den Wert **0**. Dies können Sie überprüfen, indem Sie das Beispiel-Loginskript **errorlevel.cmd** testen:

```
@echo off
net use i: /del
ifmember "Testfirma\Verkauf"
if errorlevel 1 net use I: \\s1\Verkoff
if errorlevel 2 echo Errorlevel hat den Wert 2
if errorlevel 1 echo Errorlevel hat aber auch den Wert 1
if errorlevel 0 echo Errorlevel hat aber auch den Wert 0
pause
```

Alle drei echo-Zeilen werden angezeigt. Wenn Sie jetzt **Verkoff** in **Verkauf** berichtigen und das Skript erneut durchlaufen lassen, wird nur noch die letzte echo-Zeile angezeigt.

Die Auswertung des Erfolgs oder Misserfolgs von if errorlevel-Befehlen muss also sauber durchgetestet werden.

10.9 Die Variable LOGONSERVER verwenden

Wenn Sie später mehrere Domänencontroller haben und der Server **S1** ausfällt, so würde der Befehl **\\s1\netlogon\util\ifmember.exe testfirma\Verkauf** zu einer Fehlermeldung führen. Es ist deshalb sinnvoll, statt **\\S1** die Variable **LOGONSERVER** zu verwenden. Deren Inhalt zeigt zwei Backslashs **** und den Namen des Anmeldeservers an. Außerdem ist es sinnvoll und vermeidet Fehler, wenn Sie an den Anfang des Loginskriptes den Befehl **net use L: %LOGONSERVER%\netlogon /persistent:no** stellen, weil die nachfolgenden Befehle dann kürzer ausfallen und die Gefahr von Schreibfehlern vermindert wird. Der Befehl **\\s1\netlogon\util\ifmember.exe testfirma\Verkauf** verkürzt sich dann auf **L:\util\ifmember.exe testfirma\Verkauf**. Die Routine **ifmember1.cmd** hat jetzt folgendes Aussehen:

```
net use l: %LOGONSERVER%\netlogon /persistent:no
net use g: /d
l:\util\ifmember.exe testfirma\Verkauf
if errorlevel 1 net use g: \\s1\Verkauf /persistent:no
pause
```

```
?
? "Drücken Sie eine beliebige Taste..."
get $Taste
; 5 Sekunden warten:
? "In 5 Sekunden wird eine Datei kopiert."
sleep 5
goto WEITER
? Diese Zeilen werden uebersprungen
:WEITER
copy \\S1\NETLOGON\KIX\kix32.exe g:\kix32.exe
exit
```

Drucken Sie die Hilfedateien zu Kix32 aus, um sich die vielfältigen Möglichkeiten dieses Tools zu erschließen. Trotz seiner Mächtigkeit ist die Syntax der Kix-Befehle leicht erlernbar.

10.15 SU (Switch User) nutzen, um mit beliebigen Rechten zu operieren

Das Loginskript soll aber nicht nur dazu dienen, Laufwerksbuchstaben nach Gruppenzugehörigkeit zuzuweisen. Wie am Anfang dieses Kapitels erwähnt wurde, sollen mit Hilfe des Loginskriptes beliebige Operationen und Einstellungen in der Umgebung des sich anmeldenden Benutzers, aber auch im Betriebssystem selbst vorgenommen werden, bis hin zur Deinstallation, zur Installation oder zum Update ganzer Anwendungen und natürlich zum Einspielen von Service Packs für das Betriebssystem Windows XP.

Nun läuft aber das Loginskript im Rechtekontext des sich anmeldenden Anwenders ab. Der Anwender gehört jedoch in der Regel zur Gruppe der Domänen-Benutzer und ist damit nicht berechtigt, Dateien an beliebiger Stelle der lokalen Festplatte auszutauschen, neue Verzeichnisse anzulegen, Registrierschlüssel unter HKEY-LOCAL-MACHINE zu ändern, zu löschen oder neu einzufügen oder Dienste zu installieren.

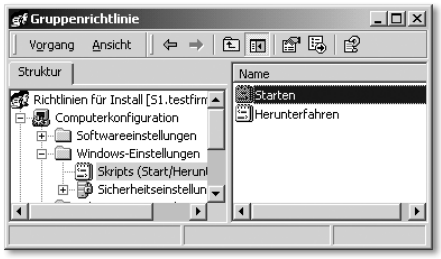
Alle diese Aufgaben können jedoch über ein zentrales Loginskript erfüllt werden, wenn man das Tool **Switch Users** (su.exe) aus dem Windows Server Resource Kit einsetzt. SU besteht aus den zwei Komponenten **su.exe** und suss.exe. Auf jeden Windows XP-Rechner müssen diese beiden exe-Dateien unter **C:\Windows\System32** eingespielt werden, und der SU-Dienst muss einmalig mit dem Befehl **suss -install** installiert werden. Diese Routine erledigt eine Batch-Datei: Die beiden exe-Dateien **se.exe** und **suss.exe** werden in das Verzeichnis **\\s1\netlogon\util** kopiert. Im Verzeichnis **\\s1\netlogon\batch** wird eine Routine **start.cmd** mit folgendem Inhalt angelegt:

```
@echo off
cls
echo Startskript wird durchgefuehrt...
if exist c:\windows\system32\su.exe goto WEITER
copy \\s1\netlogon\util\su.exe c:\windows\system32\su.exe /y >
NUL: 2>&1
copy \\s1\netlogon\util\suss.exe c:\windows\system32\suss.exe /y
> NUL: 2>&1
suss -install
:WEITER
```

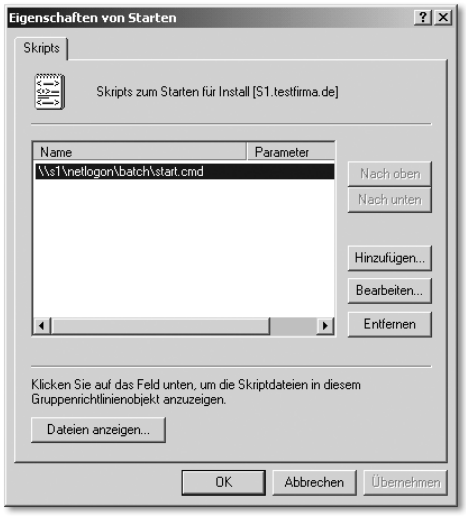
Der Parameter **/y** hinter dem copy-Befehl stellt sicher, dass eine bereits vorhandene Datei überschrieben wird, ohne dass um eine Bestätigung gebeten wird. Der Befehl **suss -install** installiert den SU-Dienst als automatisch zu startenden Dienst.

Als Nächstes erzeugen Sie mit dem Snap-In **Active Directory-Benutzer und -Computer** unterhalb der OU **Testfirma** eine neue OU **Computer** und verschieben den Windows XP-Client dorthin. Jetzt erstellen Sie für die neue OU **Computer** eine Gruppenrichtlinie: Sie stellen die Maus auf die OU **Computer**, klicken die rechte Maustaste und wählen **Eigenschaften**, dann die Registerkarte **Gruppenrichtlinien** und die Schaltfläche **Neu**. Als Namen für die neue Gruppenrichtlinie vergeben Sie **Install**. Wählen Sie nun die Schaltfläche **Eigenschaften** und dort **Benutzerdefinierte Konfigurationseinstellungen deaktivieren**. Da diese Richtlinie nur für Computer genutzt wird, jedoch keine Einstellungen für Benutzer in dieser Richtlinie gemacht werden sollen, kann die Abarbeitung der Richtlinie beschleunigt werden, wenn diese Option markiert wird.

Über die Schaltfläche **OK** verlassen Sie die Eigenschaften und wählen sofort **Bearbeiten**, um ein Startskript für alle Computer, die in dieser OU **Computer** liegen, zu aktivieren. Wählen Sie dazu unter **Computerkonfiguration · Windows-Einstellungen · Skripts (Start/Herunterfahren)** die Richtlinie **Starten**.



Geben Sie über die Schaltfläche Hinzufügen das Startskript **\\s1\netlogon\batch\start.cmd** an.



Sie müssen den Windows XP-Computer unter Umständen zweimal neu starten, damit der SU-Dienst wirklich installiert wird. Über Gruppenrichtlinien aktivierte Startskripts werden ausgeführt, sobald der PC neu startet. Es muss sich niemand an diesem PC anmelden, damit das Startskript abläuft.

Das Startskript läuft im Rechtekontext **System** ab. Somit können beliebige Aktionen ausgeführt werden. Jedoch muss der PC das erste Mal neu gestartet werden, damit er bei der Computeranmeldung an der Domäne die neue Richtlinie überhaupt übernimmt. Erst beim zweiten Start des Computers sollte dann die Richtlinie zum Tragen kommen, das Skript **start.cmd** also ausgeführt werden.

Wenn Sie beobachten möchten, wie das Startskript abläuft, müssen Sie entweder die Zeile **@echo off** deaktivieren oder eine Echo-Zeile einbauen (**echo Startskript wird abgearbeitet**) und außerdem unter **Computerkonfiguration · Administrative Vorlagen · System** die Richtlinie **Startskripte sichtbar ausführen** aktivieren.

Für das weitere Vorgehen benötigen Sie eine neue Sicherheitsgruppe **local Admins** und eine unscheinbare Kennung, die in die Gruppe **local Admins** aufgenommen wird. Legen Sie im Container **Users** die Sicherheitsgruppe **local Admins** und die Kennung **Intel** mit dem Passwort **telin1** an. Die Kennung **Intel** wird in die Gruppe **local Admins** aufgenommen und erhält kein Exchange-Postfach.

Die nächste Aufgabe besteht darin, dafür zu sorgen, dass die Domänengruppe **local Admins** in die lokale Gruppe der Administratoren aller Clients eingepflegt wird. Jeder Benutzer, der in die Gruppe **local Admins** aufgenommen wird, kann alle Computer der Organisation administrieren, ohne zur Gruppe der Domänen-Admins zu gehören. Sie können also später alle Mitglieder des Benutzersupports in diese Gruppe einpflegen. Sie können aber auch andere »Power-user« zumindest temporär in diese Gruppe aufnehmen.

Ein Beispielszenario soll die Möglichkeiten der Gruppe **local Admins** verdeutlichen: Sie haben ihre gesamte Anwendersoftware in der Freigabe **\\s1\install** auf dem Dateiserver abgelegt. Dort gibt es auch ein Verzeichnis **\\s1\install\visio**, auf das nur die Gruppe **local Admins** Leserechte hat. visio soll nur auf bestimmten Clients installiert werden. Ein Mitarbeiter, auf dessen PC bisher kein visio installiert war, soll zukünftig mit visio arbeiten. Es handelt sich um einen EDV-erfahrenen Mitarbeiter, dem Sie zutrauen, dass er sich visio selbst installieren kann. Sie nehmen den Mitarbeiter in die Domänengruppe **local Admins** auf, rufen ihn an und bitten ihn, sich mit der Freigabe **\\si1\install** zu verbinden und das Setup aus dem Unterverzeichnis

\\s1\install\visio zu starten. Sobald die Installation von visio durchgelaufen ist, entfernen Sie den Benutzer wieder aus der Gruppe **local Admins**.

Um die globale Gruppe **local Admins** der lokalen Gruppe **Administratoren** hinzuzufügen, benötigen Sie den Befehl **net localgroup Administratoren »Testfirma\local Admins« /add**. Diesen Befehl nehmen Sie in die Routine **\\s1\netlogon\batch\start.cmd** mit auf:

```
@echo off
cls
echo Startskript wird durchgefuehrt...
if exist c:\windows\system32\su.exe goto WEITER
copy \\s1\netlogon\util\su.exe c:\windows\system32\su.exe /y >
NUL: 2>&1
copy \\s1\netlogon\util\suss.exe c:\windows\system32\suss.exe /y
> NUL: 2>&1
suss -install
net localgroup Administratoren "Testfirma\local Admins" /add >
NUL: 2>&1
:WEITER
```

Der Befehl **su.exe** hat folgende Syntax: `su Kennung <Befehl>`

Der Befehl **su.exe Intel %LOGONSERVER%\netlogon\cmd\xyz.cmd** würde die Routine **xyz.cmd** mit allen in ihr enthaltenen Befehlen unter lokalen administrativen Rechten durchführen. Jedoch würde er interaktiv zuerst nach dem Passwort der Kennung **Intel** fragen. Der Befehl **echo password| su intel %LOGONSERVER%\netlogon\cmd\xyz.cmd** würde das Passwort zwar übergeben, jedoch wäre es ein Sicherheitsloch, wenn das Passwort der Kennung **Intel** in Klarschrift in einem Loginskript stünde. Jetzt kommt »Trick 17 mit Selbstüberlistung«. Dieses Problem lässt sich nämlich prinzipiell wie folgt lösen: Man erzeugt eine Batch-Routine namens **intel.bat** mit folgenden Befehlen:

```
@echo off
cls
c:
cd\
if %1.==. goto ENDE
echo telin1| su.exe intel %1 /e /1
:ENDE
```

Beachten Sie, dass zwischen dem Passwort **telin1** und dem Umleitungszeichen **|** kein Leerzeichen stehen darf.

Zuerst sorgt die Routine dafür, dass in die Root des Laufwerks **C:** gewechselt wird. Die Routine **intel.bat** wechselt ja später in den Kontext des neuen Users **Intel**. Der Kennung **Intel** sind jedoch das Laufwerk und der Pfad eventuell nicht bekannt, die zu dem Zeitpunkt aktiv sind, zu dem mittels **su.exe** in die Kennung **Intel** gewechselt wurde. Befindet sich der Benutzer, der sich anmeldet, in seinem Userhome-Directory und sind für diesen Benutzer z.B. bestimmte Netzlaufwerke wohl definiert, so gilt dieses nicht gleichsam für die Kennung **Intel**, zu der gewechselt wird. Wird aber vorher nach **C:** gewechselt, so steht auch die Kennung Intel im Verzeichnis **C:**, sobald sie mittels **su.exe** aktiviert wird.

Die Zeile **if %1.==. goto ENDE** stellt sicher, dass **su.exe** nicht ohne Angabe eines Parameters gestartet wird. Der Parameter ist später die unter der Kennung **Intel** auszuführende Routine.

Die Parameter **/e** und **/l** in der Zeile, in der das Tool **su.exe** gestartet wird, sorgen dafür, dass der Kennung **Intel** die Umgebungsvariablen der aufrufenden Kennung übergeben werden. Damit erkennt die Kennung **Intel** z.B. anschließend den Inhalt der Variablen **%LOGONSERVER%**.

Erscheint die Fehlermeldung **CreateProcessAsUser error! (rc=3)** beim Aufruf des SU-Tools, so deutet sie darauf hin, dass nicht in den Kontext des neuen Users gewechselt werden kann, weil die Umgebung, aus der gewechselt werden soll, für den neuen User nicht passt. Lesen Sie in der Dokumentation des Resource Kits unter »Switch User« nach, welche Bedeutung die einzelnen Parameter haben. Machen Sie sich generell kundig, welche Möglichkeiten SU bietet. Es ist ein mächtiges Tool!

In obiger Batch-Routine lautet das Passwort der Kennung **Intel »telin1«**. In dieser Batch-Routine steht das Passwort noch lesbar und könnte von einem pfiffigen Anwender missbraucht werden. Diese Batch-Routine wandelt man mittels des Tools **batcom.exe** in eine exe-Datei um: **batcom intel.bat**

Sie finden das Tool **batcom** auf der Buch-CD im Verzeichnis NETLOGON\Util. In der so erzeugten Datei **intel.exe** kann man das Passwort nur noch mittels eines Hexeditors einsehen. Um noch mehr Sicherheit zu bekommen, verdichtet man die erzeugte exe-Datei mit einem Tool wie **upx.exe**, das Sie ebenfalls auf der CD unter **upx intel.exe finden.**

Die mittels **upx** verdichtete Datei **intel.exe** lässt sich dann auch mit einem Hexeditor nicht mehr analysieren. Das so erzeugte Tool **intel.exe** kopiert man nach **%LOGONSERVER%\netlogon\util**.

Auf das Verzeichnis **netlogon\util** haben die Domänenbenutzer Leserechte. Auf dem Unterverzeichnis **netlogon\util\batcom** entzieht man allen Benut-

zern mit Ausnahme der Domänen-Admins die Rechte, sodass kein Anwender die ursprüngliche Routine intel.bat mit dem lesbaren Passwort **telin1** einsehen kann.

Das neu generierte Tool **intel.exe** können Sie für alle möglichen Zwecke einsetzen. Der Befehl **%LOGONSERVER%\netlogon\util\intel.exe %LOGONSERVER%\netlogon\cmd\test23.cmd** im Loginskript würde z.B. die Routine **test23.cmd** im Rechtekontext der Kennung **Intel** ausführen, also mit lokalen administrativen Rechten. Mit diesem mächtigen Werkzeug können Sie nun über das Loginskript tun, wonach Ihnen der Sinn steht. Einige Beispiele sollen nachfolgend verdeutlichen, welche Möglichkeiten Ihnen ab sofort zur Verfügung stehen.

10.16 Beispiele für die Anwendung von SU

Im Unterverzeichnis **NETLOGON\REG** der Buch-CD finden Sie die Datei **Arbeitsplatzumbenennung.reg**, die drei Schlüssel unter **HKEY_CLASSES_ROOT\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}** so umändert, dass das Desktopsymbol **Arbeitsplatz** anschließend nicht mehr die Bezeichnung **Arbeitsplatz**, sondern den Namen des aktuell angemeldeten Anwenders und dahinter den Namen des PCs trägt, z.B. **Testuser an PC0001**.

Die Datei **machinetemp.reg** verändert im Registry-Pfad **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SessionManager\Environment** die beiden Variablen **Temp** und **Tmp** derart, dass sie zukünftig nicht mehr auf **%SystemRoot\Temp** verweisen, sondern auf **C:\Temp**.

Die Datei **NoDebugFile.reg** ändert unter **[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl]** den Wert des Schlüssels **CrashDumpEnabled** in **0** ab, sodass bei einem Absturz des Rechners kein Speicherabbild mehr erzeugt wird.

Die Datei **WheelMouseErkennen.reg** erzeugt unter **HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\i8042prt\Parameters** den Schlüssel **"EnableWheelDetection"=dword:1**, wodurch eine Maus mit Rad zukünftig automatisch erkannt wird.

Alle diese Änderungen kann ein normaler Benutzer im Allgemeinen nicht durchführen, da er im Maschinenteil der Registrierdatenbank keine Änderungen durchführen darf. Mit dem erzeugten Tool **intel.exe** sind derartige Manipulationen nun möglich. Legen Sie eine Routine **hlm1.cmd** unter **netlogon\batch** mit folgendem Inhalt an (Sie finden **hlm1.cmd** auch auf der CD):

```
@echo off
cls
```

```
if exist c:\temp\NUL goto TEMPOKAY
md c:\temp > NUL
%LOGONSERVER%\netlogon\util\xcacls.exe c:\temp /e /g Benut-
zer:wc /y
regedit /s %LOGONSERVER%\netlogon\reg\machinetemp.reg
:TEMPOKAY
regedit.exe /s %LOGONSERVER%\netlogon\reg\arbeitsplatzumbenen-
nen.reg
regedit.exe /s %LOGONSERVER%\netlogon\reg\nodebugfile.reg
regedit.exe /s %LOGONSERVER%\netlogon\reg\wheelmouseerkennen.reg
```

Diese Routine erzeugt das Verzeichnis **C:\Temp**, falls es noch nicht existiert, und erteilt der lokalen Gruppe **Benutzer** die zusätzlichen Rechte »Schreiben«, »Ändern«, »Löschen«. Danach werden die oben genannten Änderungen im Schlüssel **HKEY_LOCAL_MACHINE** der Registrierdatenbank vorgenommen. Der Parameter **/s** hinter dem Befehl **regedit.exe** bewirkt, dass der Regedit-Befehl im »Silent-Mode«, d. h. ohne Aufforderung zur Bestätigung durchgeführt wird. Ohne diesen Parameter würden zwei Fenster erscheinen, und der Anwender müsste bestätigen, dass die jeweilige reg-Datei importiert werden soll.

Aktivieren Sie als Loginskript für die Kennung **Testuser** das beiliegende Skript **intel1.cmd**. Es startet die Unterroutine **NETLOGON\batch\hlm1.cmd**:

```
@echo off
cls
echo Anmeldung an der Domaene %USERDNSDOMAIN%
c:
net use L: /d > NUL: 2>&1
net use L: %LOGONSERVER%\netlogon > NUL: 2>&1
L:\util\intel.exe %LOGONSERVER%\netlogon\batch\hlm1.cmd
```

Beachten Sie, dass das erzeugte Tool **intel.exe** aus dem Verzeichnis **L:\util** aufgerufen wird, der übergebene Parameter jedoch **%LOGONSERVER%\netlogon\batch\hlm1.cmd** und nicht etwa **L:\batch\hlm1.cmd** lauten muss. Warum? Sobald mittels SU in den Kontext der Kennung **Intel** gewechselt wird, ist die Laufwerkszuweisung **net use L: %LOGONSERVER%\netlogon** nicht mehr gültig, und damit würde die Routine **L:\batch\hlm1.cmd** nicht gefunden werden kann. Denn die Laufwerkszuweisung **L:** gilt nur für den sich gerade anmeldenden Anwender, nicht aber für die Kennung **Intel**, die mittels SU aktiviert wird. Würde hier stattdessen die Zeile **L:\util\intel.exe L:\batch\hlm1.cmd** stehen, so erhielten Sie die Fehlermeldung **CreateProcessAsUser error! (rc=3)**.

Die Unterroutine **hlm1.cmd** wird somit nicht mit den Rechten des sich anmeldenden Anwenders durchgeführt, sondern mit den Rechten der Kennung **Intel**, also mit administrativen Rechten. Da die Routine **hlm1.cmd** Änderungen am Schlüssel **HKEY-LOCAL-MACHINE** vornimmt, werden diese Änderungen erst aktiv, wenn der Computer neu gestartet wird.

Durch das Aktivieren der Gruppenrichtlinie **Zugriff auf Programme zum Bearbeiten der Registrierung verhindern** unter **Benutzerkonfiguration · Administrative Vorlagen · System** können Sie übrigens verhindern, dass ein Anwender ein Registry-Tool wie **regedit.exe** überhaupt starten kann. Sie können jedoch alle benötigten Manipulationen an der Registrierdatenbank auch mittels eines Kix-Skriptes vornehmen. Kix-Befehle wie ADDKey, WriteValue, DelKey, DelTree oder DelValue funktionieren aus einem Loginskript heraus auch dann, wenn die Gruppenrichtlinie **Zugriff auf Programme zum Bearbeiten der Registrierung verhindern** aktiviert ist. Da jedoch die Routine **hlm1.cmd** im Kontext des Benutzers **Intel** abläuft und da sich diese Benutzerkennung im Container **Users** befindet, stört die Gruppenrichtlinie in diesem Fall solange nicht, wie Sie die Gruppenrichtlinie nur auf die OU **Testfirma** und nicht auf den Container **Users** anwenden.

Zum Lieferumfang von Windows XP gehören auch die Tools **regini.exe** und **reg.exe**. Beide Tools werden bei der Installation in das Verzeichnis **c:\windows\system32** eingespielt. Beide Tools finden Sie übrigens auch im Windows Server Resource Kit. Dort sind diese Tools und viele weitere Registrierdatenbank-Tools in ihrer Funktionsweise ausführlich beschrieben. Zu **regini.exe** finden Sie dort eine **regini.doc**. Die Parameter des Tools **reg.exe** erhalten Sie über den Befehl **reg.exe /? > c:\reg.txt**.

10.17 Ein zentrales Verzeichnis für temporäre Dateien anlegen

Wenn Sie als Administrator bereits weitere Programme auf dem PC installiert haben, werden Sie unter **C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temp** wahrscheinlich eine Menge weiterer Verzeichnisse finden, die mit **_ISTMP?.DIR** beginnen. Überprüfen Sie bei dieser Gelegenheit einmal, welcher »Datenschrott« sich jeweils unter den Kennungen **C:\Dokumente und Einstellungen\Kennung \Lokale Einstellungen\Temp** oder **...Lokale Einstellungen\Temporary Internet Files** angesammelt hat. Windows XP legt wie sein Vorgänger Windows 2000 für jeden Anwender, der sich anmeldet, ein separates Temp-Verzeichnis und ein separates Verzeichnis für Temporary Internet Files an. Das gilt übrigens auch auf für die Windows Server-Versionen! Je mehr Anwender sich mit unterschiedlichen Kennungen

Das Skript ist durch REM-Zeilen ausreichend dokumentiert, so dass jeder Administrator der Organisation jederzeit nachvollziehen kann, was dort geschieht. Sensible Befehle wie diejenigen, die mittels des SU-Befehls administrative Dinge ausführen, sind allerdings nicht kommentiert. Ein zu neugieriger Anwender soll schließlich nicht erfahren, wie er sich administrative, lokale Rechte auf seinem Computer verschaffen kann.

Wenn das Skript bei Ihnen Fehlermeldungen anzeigt oder bestimmte Ergebnisse nicht eintreffen, gehen Sie wie folgt vor:

Kommentieren Sie die Zeile **@echo off** aus (REM @echo off) und fügen Sie an mehreren Stellen pause-Befehle ein. Sie können so eingrenzen, wo im Skript etwas schief läuft. Wahrscheinlich werden Sie dann auch noch die Umleitung der Befehlsmeldungen **> NUL« bzw. »> NUL: 2>&1** deaktivieren müssen, damit Sie die Fehlerquelle feststellen können.

Durch den Aufruf der Unterroutine **hlm.cmd** wird ein zweites Fenster geöffnet. Das sieht zugegebenermaßen ein wenig unschön aus. Sie können jedoch später, wenn das Skript hlm.cmd fehlerlos läuft, mittels des start-Befehls versuchen, diese Unterroutine in einem minimierten Fenster laufen zu lassen. Die Syntax **start /min <Befehl>...** ermöglicht so etwas. Geben Sie den Befehl **start /?** ein, um sich die möglichen Parameter des Befehls **start** und deren Bedeutung anzeigen zu lassen.

10.28 Visual Basic-Skripte verwenden

Sie können Ihr gesamtes Loginskript auch mit Visual Basic erstellen oder aber bestimmte Unterroutinen als VBS-Dateien aufrufen. Dazu benötigen Sie nur einen Editor wie Notepad.

Im Unterverzeichnis Netlogon\VBS finden Sie folgende Beispielskripte:

- `AlleDateienEinesOrdnersLoeschen.vbs`
- `Anzeigen-der-Versionen-von-WSH-VBScript-WMI-ADSI.vbs`
- `Benutzer-aus-Gruppe-loeschen.vbs`
- `BenutzerkontoAttributeAendern.vbs`
- `Benutzerkonto-Attribute-setzen.vbs`
- `BenutzerkontoErstellen.vbs`
- `Benutzerkonto-im-AD-loeschen.vbs`
- `BenutzerProfileKonfigurieren.txt`
- `BenutzerProfilKonfigurieren.vbs`
- `Computerkonto-in-OU-verschieben.vbs`
- `Computerkonto-umbenennen.vbs`

- DateiLoeschen.vbs
- Datei-verschieben.vbs
- Dienst-intallieren.vbs
- Dienst-loeschen.vbs
- Dienst-starten-und-alle-abhaengigen-Dienste.vbs
- Dienst-stoppen-und-alle-abhaengigen-Dienste.vbs
- Drucker-installieren-aus-Treiberverzeichnis.vbs
- DruckerLoeschen.vbs
- GlobaleGruppeErstellen.vbs
- GlobaleGruppenErstellen.vbs
- Gruppe-im-AD-loeschen.vbs
- GruppeVerschieben.vbs
- MapNetworkShare.vbs
- Nachricht-senden.txt
- Nachricht-senden.vbs
- Nachricht-senden2-ohne-SMTP-Dienst.vbs
- Nachricht-senden-ohne-SMTP-Dienst.vbs
- NetzdruckerVerbinden.txt
- NetzdruckerVerbinden.vbs
- NetzfreigabeErstellen.txt
- NetzfreigabeErstellen.vbs
- NeuenOrdnerErstellen.vbs
- OfficeXP-auf-lokalem-Computer-installieren.vbs
- OfficeXP-deinstallieren.vbs
- OrdnerErstellen.vbs
- OrdnerFreigabeLoeschen.vbs
- OrdnerLoeschen.vbs
- OrdnerMitUnterordnernLoeschen.vbs
- Ordner-verschieben.vbs
- OUerstellen.vbs
- OUloeschen.vbs
- OUundGruppeundBenutzerErstellen.vbs
- Software-auf-lokalem-Computer-installieren.vbs
- Software-auf-RemoteComputer-installieren.vbs
- Software-deinstallieren.vbs

Im Verzeichnis »Scripting« der Buch-CD finden Sie interessante Artikel zum Thema »Scripting« sowie Hinweise auf interessante Quellen im Internet. VB-Skripte können wie CMD-Routinen verschlüsselt werden. Ein Skript zum Verschlüsseln von VB-Skripten finden Sie ebenso auf der Buch-CD. Der Artikel

»Running Programs From WSH Scripts« (http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/scripts/sg1102.asp) aus der Artikel-Serie »The Scripting Guys« (http://www.microsoft.com/technet/columns/scripts/sgwho.asp) beschreibt, wie ausführbare Dateien (EXE, COM, CMD) aus einem VB-Skript heraus gestartet werden können.

VB-Skripte können eine Menge leisten, speziell bei Operationen im Active Directory. Denken Sie aber daran, dass das Active Directory eine »sensible Kiste« ist. Zerschießen Sie durch Testskripte nicht ihre Produktivumgebung! Testen Sie ihre Skripte in einer Testdomäne sorgfältig aus.

Wenn Sie übrigens Exchange Server installiert haben, stehen Ihnen im erweiterten Snap-In **Active Directory-Benutzer und -Computer** einige weitere Registerkarten zur Verfügung. Dazu müssen Sie unter **Ansicht** die **Erweiterten Funktionen** auswählen. Sie sehen dann bei einem Benutzer die Registerkarten **Exchange · Allgemein**, **Exchange · Erweitert**, **E-Mail-Adressen**, **Exchange-Features** und **Objekt**. Die Registerkarte **Objekt** zeigt Ihnen den voll qualifizierten Domänennamen des Objekts an. Wenn dort etwas wie **testfirma.de/Test-OU/Mustermann, Karl** steht, funktionieren einige Skripte nicht, da sie mit dem Komma zwischen dem Nachnamen und dem Vornamen nicht zurechtkommen.

Das Problem rührt wahrscheinlich daher, dass Sie mittels **ADSI Edit** im **Configuration Container** unter **Display-Specifier CN=407**, **CN=User-Display** unter **Property - createDialog** im Eingabefeld **Edit Attribute** die Formel **%<sn>, %<givenName>** eingetragen haben, damit zukünftig beim Anlegen neuer Benutzer der Anzeigename nicht mehr in der Form »Vornamen Zuname« erscheint, sondern in der Form »Zuname, Vorname«. Verlassen Sie dann die Eigenschaften des Benutzers **Mustermann**, klicken Sie die Kennung **Mustermann, Karl** mit der rechten Maus an, wählen Sie **Umbenennen** und geben Sie der Kennung einen Namen wie **Mustermann** oder **MustermannK**. Der Anzeigename **Mustermann, Karl** bleibt davon unberührt, aber das VB-Problem ist gelöst. Weitere Hinweise zu diesem Problem finden Sie auf der Begleit-CD des Buches.

Übernehmen Sie dazu vom beiliegenden Datenträger die Routine **acrobat.cmd** nach **\\s1\netlogon** sowie die Routine **batch\acrobat.cmd** nach **\\s1\netlogon\batch\InstallAcrobat.cmd**. In der Registerkarte Profil des Benutzers **Testuser** tragen Sie hinter Loginskript das neue Loginskript **acrobat.cmd** ein. Es hat folgenden Inhalt:

```
@echo off
cls
echo Anmeldung an der Domaene %USERDNSDOMAIN%
c:
net use l: /d > NUL: 2>&1
net use l: %LOGONSERVER%\netlogon > NUL: 2>&1
net use u: /d > NUL: 2>&1
net use u: \\s1\install > NUL: 2>&1
if not exist "c:\programme\Adobe\Acrobat 5.0\Rea-
der\AcroRd32.exe" l:\util\intel.exe %LOGONSERVER%\netlo-
gon\batch\InstallAcrobat.cmd
```

Die unter der Kennung **Intel** mit den Rechten eines lokalen Administrators ablaufende Unterroutine **netlogon\batch\InstallAcrobat.cmd** hat folgenden Inhalt:

```
@echo off
cls
c:
net use u: /d > NUL: 2>&1
net use u: \\s1\install > NUL: 2>&1
u:\AcrobatReader.505\setup -s
```

Die **setup.exe** des Acrobat Readers wird also mit dem Parameter **-s** für eine unbeaufsichtigte Installation gestartet: Sie läuft im Hintergrund ab, ohne dass Fenster erscheinen, die Benutzereingaben verlangen. Es dauert einige Zeit, bis die Installation abgeschlossen ist, und Sie die Verknüpfung **Acrobat Reader 5.0.lnk** sowohl unter **C:\Dokumente und Einstellungen\All Users\Desktop** als auch unter **C:\Dokumente und Einstellungen\All Users\Startmenü\Programme** finden.

11.4 Microsoft Office automatisch installieren

Zum Zeitpunkt der Erstellung dieses Kapitels gab es zur Beta-Version von Microsoft Office 2003 noch kein Office 2003 Resource Kit. Ebenso lagen die Gruppenrichtliniendateien von Office 2003 noch nicht vor. Ohne die Tools des Resource Kits und die Gruppenrichtliniendateien ist jedoch eine automatisierte Installation von Office 2003 nicht oder nur eingeschränkt möglich. Nachfol-

gend wird deshalb die automatisierte Installation von Office XP beschrieben, da die Erkenntnisse hierfür abgesichert sind. Unter Office 2003 werden die zu verwendenden Methoden jedoch dieselben sein.

Wenn Sie nicht im Besitz eines Organisationskeys für Windows XP Professional oder Office XP sind und folglich das Betriebssystem und Office XP auf jedem einzelnen Computer aktivieren müssen, so können Sie später bei jedem Computer, auf den ein Abbild eingespielt wurde, ein Tool wie den Keyfinder (www.magicaljellybean.com/keyfinder.shtml) verwenden, um den Produkt-Key nachträglich zu ändern und das Betriebssystem dann über das Internet zu aktivieren. Mit dem Tool **keyfinder.exe** kann man sich außerdem den Produkt-Key von Office XP anzeigen lassen, ihn aber leider nicht verändern.

Wenn Sie übrigens den gesamten Schlüssel **[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\10.0\Registration\{90280407-6000-xxxx-8CFE-0050048383C9}]** mit den zugehörigen Unterschlüsseln **Product-ID** und **DigitalProduct-ID** löschen, so werden Sie beim nächsten Start von Word aufgefordert, den Namen des Benutzers, den Organisationsnamen und den Produkt-Key erneut einzugeben. Dadurch wird der Schlüssel erneut erstellt.

Interessant sind in diesem Zusammenhang die Dateien **OEM2.DOC**, **OEM.BAT** und einige Tools, die man auf einer Microsoft Office XP OEM Preinstallation Kit-CD findet. Diese CD wird für die Vorinstallation von Office XP durch Systembuilder ausgeliefert. Die **OEM.BAT** wird mit einem Parameter wie **PRO** für Professional oder **OUTLOOK** aufgerufen. Danach wird unter anderem eine Variable namens **_OPSProductCode** gesetzt und dem Tool **srclist.exe** übergeben. Anschließend ist der oben genannte Schlüssel gelöscht, und beim ersten Start einer Office-Komponente wird der Benutzer zur Eingabe des Produkt-Keys aufgefordert.

Suchen Sie unter www.google.de nach den Begriffen »keyfinder«, »OEM Preinstallation Kit« oder »Preinstallation Office XP«. Unter http://members.microsoft.com/partner/products/windows/windowsxp/Windows_XP_Tools_e.aspx finden Sie den Artikel »Windows XP Preinstallation Tools and Documentation« und unter http://members.microsoft.com/partner/products/windows/windowsxp/Preinstallation_Checklist.aspx eine Checkliste zur Vorinstallation von Windows XP.

Mir gefällt es überhaupt nicht, dass Anwendungen wie der Acrobat Reader oder Winzip ihre Icons auf dem Desktop, direkt über dem Start-Button oder

direkt unter **C:\Dokumente und Einstellungen\Programme** ablegen. Ich verbanne diese nebensächlichen Anwendungssymbole deshalb nach **C:\Dokumente und Einstellungen\All Users\Programme\Zubehör**. Wie das geht, zeige ich Ihnen, nachdem Microsoft Office XP Standard über das Loginskript installiert wurde.

Legen Sie unter **\\s1\install** ein Verzeichnis **Office.XP** an. Starten Sie auf dem Server **S1** von der Office-CD das Setup mit dem Parameter **/a** für eine Administrative Installation. Besorgen Sie sich das Administrative Office XP Service Pack 2 von http://download.microsoft.com/download/officexpstandard/sp/oxpsp2/w98nt42kmexp/en-us/oxpsp2a.exe. Das Service Pack 1 wird bei einer administrativen Installation von Office XP nicht mehr benötigt. Entpacken Sie die Datei **oxpsp2a.exe** nach **c:\oxsp2a** und setzen Sie folgenden Befehl ab:

msiexec /a Laufwerk:\install\office.xp\proplus.msi /p c:\oxsp2a\mainsp2ff.msp SHORTFILENAME=1 /qb+

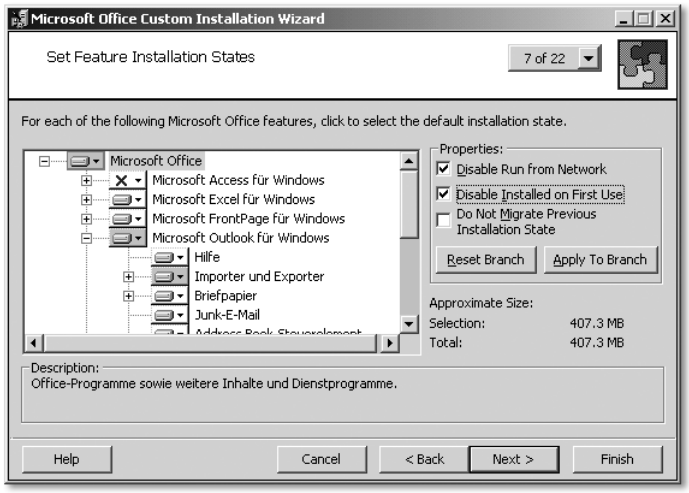
Dadurch wird das Service Pack 2 in Ihre Administrative Office XP-Installation integriert. Diese Vorgehensweise ist im Knowledge Base-Artikel »Q325671 – Overview of the Office XP Service Pack 2 (SP-2)« beschrieben. Installieren Sie auf dem Server **S1** das Office XP Resource Kit. In einer Produktivumgebung sollten Sie natürlich das Office XP Resource Kit nicht auf dem Server installieren, sondern auf einem Computer mit Windows XP. Da unsere Testumgebung aber nur aus einem Server namens **S1** und einem Musterclient mit Windows XP besteht und der Musterclient als Vorlage für ein Komplettabbild dienen soll, dürfen dort keine Anwendungen installiert werden, die später nicht auf alle Computer ausgerollt werden dürfen. Deshalb behelfen wir uns in der Testumgebung und installieren das Office XP Resource Kit auf dem Server.

Hinweis Wenn Sie bei der Auswahl der zu installierenden Komponenten die **Vollständige Installation** auswählen, wird auch Microsoft IEAK installiert. Es gibt jedoch bereits eine neuere Version des Internet Explorer Administration Kits. Sie finden diese neue Version unter http://www.microsoft.com/windows/ieak/de/default.asp.

Starten Sie aus den Microsoft Office XP Resource Kit Tools den **Custom Installation Wizard** und geben, wenn Sie nach einer MSI-Datei gefragt werden, die Datei **\\s1\install\Office.XP\ProPlus.MSI** an. Erzeugen Sie im Administrativen Installationspunkt **\\s1\install\Office.XP** eine neue Transformationsdatei mit dem Namen **Standard.MST** für Office XP. Geben Sie als **Organization Name** den Namen der Organisation an (z. B. **Testfirma**).

Im nächsten Fenster **Remove Previous Version** übernehmen Sie die Vorauswahl **Default Setup behavior**. Diese Voreinstellung deinstalliert eine eventuell vorhandene Office-Installation, bevor die neue Installation beginnt.

Im folgenden Fenster **Set Feature Installation States** können Sie die zu installierenden Komponenten auswählen.



Wichtig ist, dass keine Komponenten vom Server gestartet oder später beim ersten Aufruf nachinstalliert werden. In einem komplexen Netzwerk mit mehreren Standorten könnte es zu Problemen führen, wenn ein Client versucht, über eine langsame WAN-Verbindung auf einen Server zuzugreifen, der nicht am jeweiligen Standort steht, um eine Komponente nachzuinstallieren oder gar vom Server zu laden.

Da die Festplatten in Computern heute so dimensioniert sind, dass der Speicherplatz in der Regel kein Problem mehr darstellt, wählen Sie besser zu viele Komponenten aus, als später feststellen zu müssen, dass eine abgewählte Komponente doch benötigt wird und aufwendig auf hunderten von Computern nachinstalliert werden muss. Seien Sie also nicht zu restriktiv! Wählen Sie keine Komponente ab, wenn Sie sich nicht sicher sind, dass diese Komponente später bei der Erweiterung des Netzwerks (z.B. durch die Einführung neuer Produkte wie Microsoft Conferencing Server oder die Integration der Telefonanlage in den Exchange Server) doch benötigt werden. Im Zweifelsfall wählen Sie alle Komponenten aus, indem Sie **Alles vom Arbeitsplatz starten** als Option wählen.

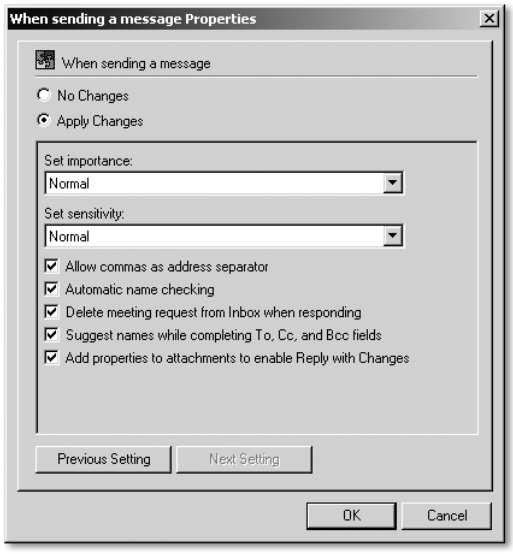
Eine Komponente sollten Sie jedoch auf jeden Fall abwählen: Die **Microsoft Office Shortcut-Leiste** unter Office Tools. Da alle Office-Komponenten kom-

fortabel über das Startmenü oder die Taskleiste gestartet werden können, ist die Office Shortcut-Leiste für den Anwender nur verwirrend. Sie ist auch schon standardmäßig auf **nicht verfügbar** gesetzt. Wahrscheinlich hat Microsoft inzwischen erkannt, dass die Shortcut-Leiste mehr Verwirrung als Nutzen stiftet und viel zu kompliziert zu konfigurieren ist.

Markieren Sie **Disable Run from Network** sowie **Disable Installed on First Use** und klicken Sie dann auf **Apply To Branch**, damit sichergestellt ist, dass keine Teilkomponenten vom Netzwerk gestartet oder beim ersten Aufruf aus dem Startmenü nachinstalliert werden.

Als nächstes Fenster erscheint ein Hinweis, dass eine OPS-Datei integriert werden kann. Diese OPS-Datei kann vor dem Aufruf des **Custom Installation Wizard** mit dem Office Resource Kit Tool **Profil Wizard** erzeugt werden und wichtige Office-Defaulteinstellungen wie z.B. den Namen des Standard Exchange Servers aufnehmen.

Im nächsten Fenster können Sie viele Voreinstellungen für Office-Komponenten vornehmen. Leider sind die Optionen nicht erklärt. Hier hilft nur eins: Installieren Sie Office XP mit allen Komponenten auf einem separaten Computer und starten Sie dort die einzelnen Komponenten. Wählen Sie für jede Anwendung **Extras · Optionen** und sehen Sie sich die Hilfetexte zu den einzelnen Optionen direkt unter einem installierten Office XP an.



Sie sollten unter **Preferences · e-mail options · Advanced e-mail options-when sending a message** einstellen, dass neben dem Semikolon auch das Komma als Trennzeichen zugelassen wird.

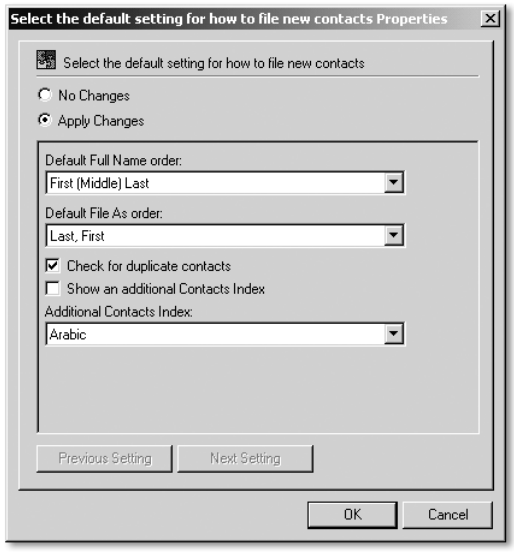
Diese Einstellung bewirkt, dass der Anwender später bei der Erstellung einer neuen Nachricht im Feld **An** zwei Empfänger-Kennungen wie **schlueter**, **rath** durch ein Komma getrennt eingeben kann und Outlook bei der Namensauflösung diesen Eintrag dann als zwei Empfänger interpretiert und nicht als »Nachname, Vorname«.

In einem Büro mit mehreren Mitarbeitern ist es bestimmt unangebracht, wenn bei der Ankunft einer neuen Nachricht der Lautsprecher aktiv wird. Deaktivieren Sie deshalb unter **When new items arrive** die Option **Play a sound**.

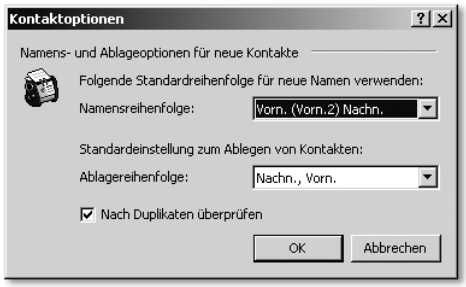
Unter **Calendar Options** sollten Sie die **Working hours** konfigurieren, indem Sie die Arbeitszeiten Ihres Unternehmens eintragen. Sicherlich ist es auch sinnvoll, wenn unter **Calender week numbers** die Anzeige der Wochennummern aktiviert wird.

Die Option **Allow attendees to propose new times for meetings you organize** ist identisch mit der Option **Teilnehmer dürfen andere Besprechungszeiten vorschlagen** und sollte aktiviert werden.

Aktivieren Sie unter **contacts options** die Option **Check for duplicate contacts**.



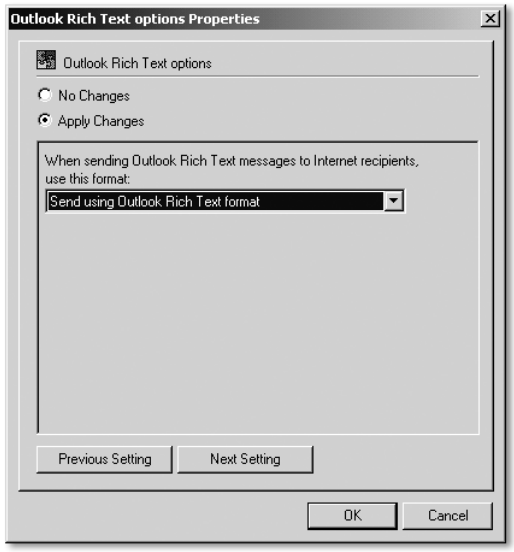
In den Optionen von Outlook wird dadurch bei einem neuen Anwender in den Kontaktoptionen die Option **Nach Duplikaten überprüfen** aktiviert.



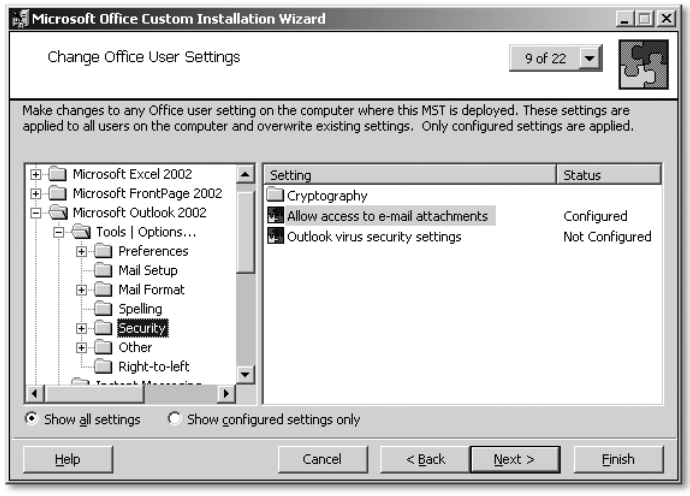
Die Journaloptionen sollten als Voreinstellung für einen neuen Anwender **nicht konfiguriert** bleiben. Die Journalfunktion wird von den wenigsten Anwendern aktiv genutzt. Sie ist aber ressourcenintensiv.

Unter **Mail Format · Message Format** können Sie darüber nachdenken, die Voreinstellung **Use Microsoft Word to read rich text e-mail messages** zu deaktivieren. In früheren Office-Versionen waren die Editierfunktionen von Outlook sehr beschränkt, sodass es sinnvoll war, als Editor für Nachrichten jedes Mal Word zu starten. Inzwischen ist jedoch der in Outlook integrierte Nachrichteneditor mächtig genug, um auch **Reach Text Messages** zu schreiben und erhaltene Nachrichten fehlerfrei und sauber formatiert darzustellen, ohne dass Word hinzugeladen werden muss.

Da alle gängigen E-Mail-Produkte inzwischen keine Probleme mehr haben, mit dem erweiterten Zeichensatz umzugehen, können Sie außerdem unter **Mail Format · Internet Formatting** die Option **Outlook Rich Text options** von **Convert to plain text format** umstellen in **Send using Outlook Rich Text format**.



In den Security-Seetings können Sie über den Menüpunkt **Allow access to e-mail attachments** einstellen, welche Dateianhänge in Outlook zugelassen sind.



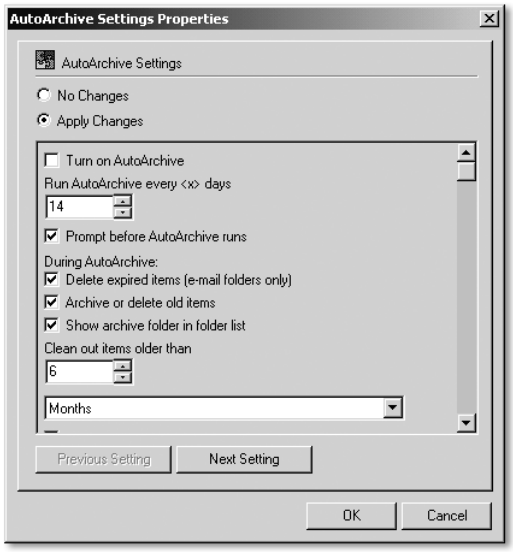
Microsoft hat mit dem Aufkommen immer neuer Virentypen seit dem Erscheinen des Service Pack 2 zu Office 2000 per Standardeinstellung die Typen der erlaubten Mail-Anhänge stark eingeschränkt. Diese Voreinstellung ist für unbedarfte Privatanwender sicherlich sinnvoll, da auf Heimcomputern oft kein aktueller Virenscanner und auch keine Firewall installiert sind. In Firmennetzen sieht das jedoch anders aus. In der Regel gibt es nur einen oder wenige Zugänge zum Internet, die durch Firewalls abgesichert sind. Auf den Mailservern und auf den Dateiservern laufen Virenscanner, die ständig aktualisiert werden. Für den Exchange Server gibt es Antivirenprodukte, die neue Nachrichten inklusive ihrer Dateianhänge bereits auf Viren untersuchen, bevor sie in die Exchange-Datenbank übernommen werden. Wenn aber bestimmte Arten von Anhängen nicht mehr geöffnet werden dürfen, so kann das auch kontraproduktiv sein. So können Sie dann z. B. öffentliche Exchangeordner nur noch eingeschränkt nutzen und keine Access-Datenbank mit einer Literaturdatenbank hinterlegen. Denn der Anwender könnte sie nicht öffnen. Eine andere Möglichkeit, bestimmte Dateinamensendungen für Nachrichtenanhänge wieder in Outlook zugänglich zu machen, als die, diese Dateinamensendungen bereits über den **Microsoft Office Custom Installation Wizard** freizugeben, wird an anderer Stelle dieses Buches erörtert.

Interessant ist in diesem Zusammenhang aber die Option **Apply individual Settings for Outlook virus security**, die standardmäßig deaktiviert ist und hier aktiviert werden kann.

In der Kattegorie **Outlook 2002 · Tools · Other** sollten die Optionen **Empty Deleted Intems Folder** sowie **Make Outlook the default program for E-Mail, Contacts and Calendar** aktiviert werden. In den **Advanced Options** sollte zusätzlich die Option **Warn before permanently deleting items** deaktiviert werden. So ist sichergestellt, dass beim Beenden von Outlook die gelöschten Objekte ohne Warnung endgültig gelöscht werden. Die Postfächer der Anwender auf dem Exchange Server laufen dann nicht voll. Ohne diese Einstellungen bleiben alle gelöschten Nachrichten inklusive der mitgeschickten Anhänge im Ordner **gelöschte Objekte** erhalten und belegen unnötig Platz in der Exchange-Datenbank. Sie können im System-Manager des Exchange Servers einstellen, dass gelöschte Objekte erst nach einer bestimmten Anzahl von Tagen endgültig gelöscht werden. Bis dahin kann ein Anwender ein versehentlich gelöschtes Objekt jederzeit wieder herstellen: Er öffnet den Ordner **Gelöschte Objekte** und wählt über den Menüpunkt **Extras** den Befehl **Gelöschte Elemente wiederherstellen**. Ist die voreingestellte Zeit, bis zu der gelöschte Objekte auf dem Exchange Server wieder herstellbar sind, verstrichen, so können Sie im Notfall das Postfach des betroffenen Anwenders von einem alten Sicherungsband zurücksichern.

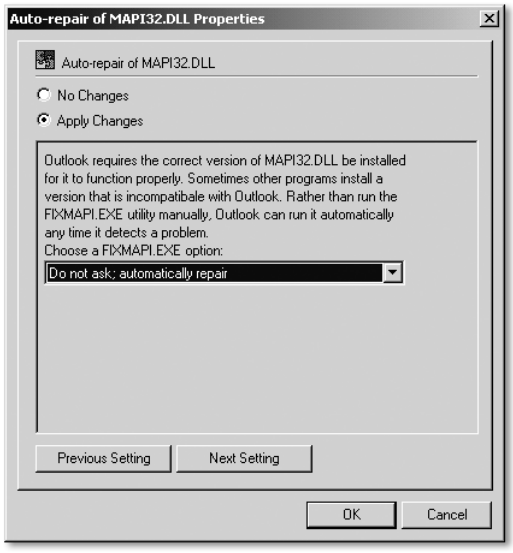
Unterhalb von **Advanced** finden Sie in den **Reminder Options** die Möglichkeit, den Lautsprecher für die Erinnerungsfunktion abzuschalten. Dies erscheint besonders dann sinnvoll, wenn mehrere Anwender in einem Büro sitzen oder Kundenkontakt haben. Das ständige Tönen des Computerlautsprechers ist für die Sachbearbeiter und die anwesenden Kunden wahrscheinlich eher lästig als hilfreich.

In der Kategorie **Auto Archive** schlage ich vor, die Autoarchivierung abzuschalten. Der einfache Anwender wird mit der Funktion **Autoarchivierung** wahrscheinlich überfordert sein. Wenn Sie die Autoarchivierung nicht deaktivieren, müssen Sie sich Gedanken machen, wie der Speicherort und der Name der Archivierungsdatei so vordefiniert werden kann, dass die Archivdatei in die tägliche Sicherung mit eingeht. Wenn die Mitarbeiter nicht regelmäßig alte Outlook-Objekte löschen, sondern diese außerhalb der Datenbank des Exchange Servers archivieren, so müssen Sie in den Speicherplatz auf dem Dateiserver investieren, um diese immer größer werdenden Archivdateien unterbringen zu können. Warum dann nicht gleich in den Speicherplatz des Exchange Servers investieren und die Maximalgröße der Postfächer erweitern?



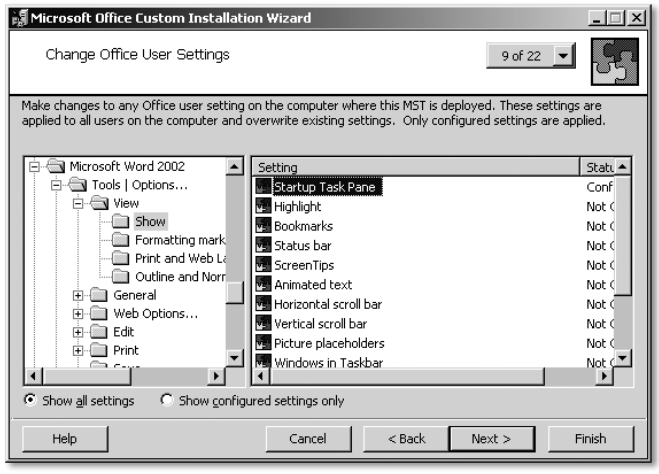
Denken Sie darüber nach, ob **Netmeeting** über die Kategorie **Miscellaneous** komplett deaktiviert werden sollte, denn **Netmeeting** wird wahrscheinlich in Ihrer Organisation nicht genutzt und zukünftig von Microsoft nicht mehr weiterentwickelt. An die Stelle von **Netmeeting** tritt **Instant Messaging** bzw. der **Conferencing Server**.

Die Option **Auto-repair of MAPI32.DLL** sollte von **Ask user before running FIXMAPI.EXE** auf **Do not ask; automatically repair** umgestellt werden.



Es erscheint auch sinnvoll, zu verhindern, dass Anwender **HTTP e-mail accounts** in einer reinen Exchange-Umgebung selbstständig hinzufügen können. Sie können dies über die Option **Prevent users from adding HTTP e-mail accounts** unterbinden.

Sowohl unter den Optionen von Word als auch unter denen von Excel und Powerpoint können Sie jeweils unter **View** die Option **Startup Task Pane** so voreinstellen, dass die **Startaufgaben** nicht als Spalte rechts erscheinen, wenn Word, Excel oder Powerpoint gestartet werden. Ich empfinde diesen Aufgabenblock, der bei jedem Start von Word oder Excel erscheint, eher störend, da er einen großen Teil des Bildschirms belegt.



Die Anzahl der Optionen, die Sie für Word, Excel, Powerpoint und Access einstellen können, ist sehr umfangreich. Sie sollten auf einem separaten Computer die einzelnen Anwendungen starten und über den Menüpunkt **Extras · Optionen** unter Verwendung der Hilfefunktion die Bedeutung der einstellbaren Optionen überprüfen.

Mit scheint es zumindest ratsam, die Funktion **Schnellspeicherung** von Word durch die Auswahl von **Apply Changes** und das Nichtaktivieren der Option **Check to turn setting on** abzuschalten, weil die Schnellspeicherung Textänderungen in der geänderten Datei hinten anhängt, statt die Datei komplett neu abzuspeichern. Außerdem können Sie die Funktion **Always create backup copy** nicht aktivieren, wenn die Schnellspeicherung zugelassen ist.

Eine weitere sehr interessante Voreinstellung ist **Prompt for document properties** in der Kategorie **Save**. Durch die Aktivierung dieser Option wird der Benutzer beim erstmaligen Speichern eines neuen Word-Dokuments automatisch mit dem Fenster **Dateieigenschaften** konfrontiert und aufgefordert, die Felder **Titel**, **Thema**, **Stichworte**, **Kategorie**, **Kommentare** und **Autor** auszufüllen. Besonders in einer gemeinsamen Gruppenablage ist es hilfreich, wenn diese Felder ausgefüllt sind und jeder Mitarbeiter anhand der Dateiinformationen schon beim Auflisten der Dateien im Windows Explorer die Bedeutung des Dokuments erahnen kann. Das hilft, in einer Fülle von Dokumenten schnell das gesuchte Dokument zu finden.

Mit der Option **Save AutoRecover info** können Sie außerdem das Zeitintervall einstellen, nach dem ein in Bearbeitung befindliches Dokument spätestens wieder gespeichert wird, um bei Ausfall der Hardware den Verlust zu begrenzen.

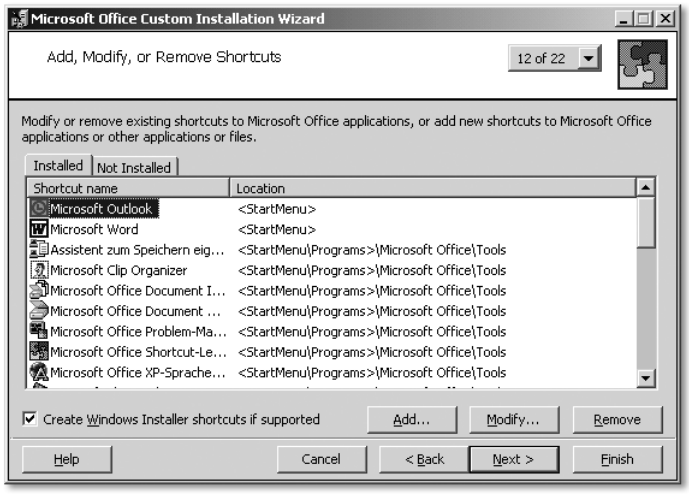
Wenn Sie in der Kategorie **Microsoft Office XP (User) · Tools · Customize** die Option **Always show full menus** aktivieren, werden die Menüs wieder vollständig angezeigt, und nicht nur die Menüpunkte, die der Anwender oft verwendet. Außerdem ist es möglich, an diversen Stellen jeweils im Fenster **Change Office User Settings** einzustellen, ob VBA oder Makros aus Sicherheitsgründen zugelassen werden sollen und wie beim Öffnen von nicht signierten Makros verfahren werden soll.

Wenn das Fenster **Add, Modify, or Remove Shortcuts** erscheint, stellen Sie ein, dass wichtige Icons wie **Microsoft Outlook** und **Microsoft Word** im Startmenü des Anwenders direkt über der Schaltfläche **Start** erscheinen, weil diese Anwendungen ständig benötigt werden und schnell gestartet werden sollen, d. h. nicht über den Umweg eines Untermenüs. Die Startmenü-Icons aller anderen Office-Hauptkomponenten, die standardmäßig unter **Start ·**

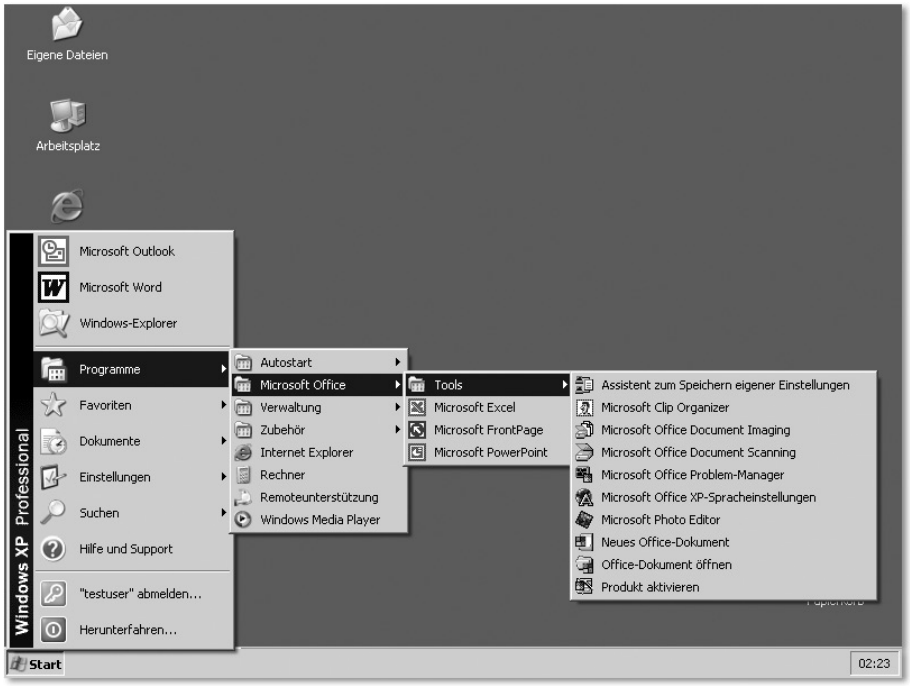
Programme stehen, verschieben Sie in ein neu erzeugtes Untermenü **Start · Programme · Microsoft Office XP**.

Die Icons, die standardmäßig unter **Start · Programme · Microsoft Office Tools** erscheinen, verschieben Sie unter **Start · Programme · Microsoft Office XP · Tools**.

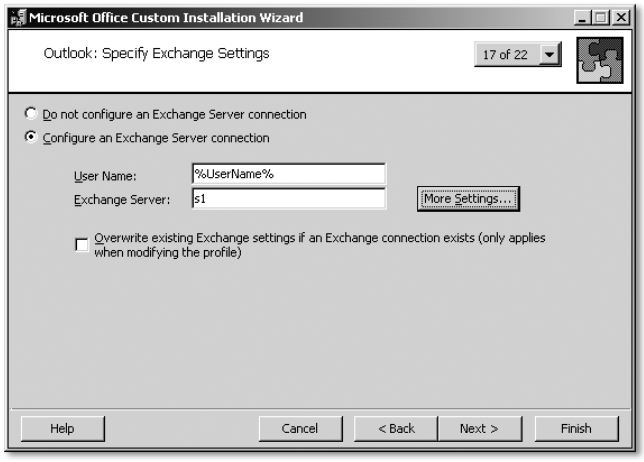
Nicht benötigte Icons wie **Office Shortcut-Leiste** und **Microsoft Office** löschen Sie. Die Verknüpfung **Microsoft Office** wird standardmäßig unter **Start · Programme · Autostart** erzeugt, belegt aber nur unnötigen Hauptspeicher.



Da sich auch in Ihrem Unternehmen nicht alles um Microsoft Office dreht, sondern kaufmännische Anwendungen oder Grafikanwendungen wie AutoCad beim Standardanwender die Arbeit bestimmen, können Sie über das Fenster **Add, Modify or Remove Shortcuts** das Startmenü übersichtlich gestalten.



Betätigen Sie im Assistenten **Custom Installation Wizard** die Schaltfläche **Next** nun so oft, bis das Fenster **Outlook: Specify Exchange Settings** erscheint. Dort können Sie den Namen des Exchange Servers eingeben und über die Variable **%UserName%** festlegen, dass bei einem Anwender, dessen Kennung und Exchange-Postfach neu erstellt wurde und der zum ersten Mal Outlook startet, automatisch das richtige Postfach gefunden wird.



Im dann folgenden Fenster **Outlook: Add Accounts** können Sie die gewünschten Exchange-Dienste konfigurieren. Es reicht wahrscheinlich, wenn zusätzlich zum Exchange-Dienst selbst nur das Outlook Adressbuch verfügbar ist. Ein persönlicher Ordner (PST-Datei) wird, wenn überhaupt, nur bei Laptop-Benutzern benötigt und sollte dann manuell hinzuinstalliert werden.

Im Fenster **Outlook: Customize Default Settings** schlage ich Ihnen vor, Outlook statt Word als Default-Editor für Nachrichten einzusetzen und die Option **Default e-mail format** von **html** in **rich text** abzuändern. Wenn Ihre Anwender mit externen Empfängern korrespondieren und diese Empfänger ein E-Mail-Programm einsetzen, dass das HTML-Format nicht unterstützt, vermeiden Sie damit Formatierungsverluste.

Wählen Sie die Schaltfläche **Next** solange, bis das letzte Fenster **Save Changes** des Assistenten angezeigt wird. Sobald Sie auf **Finish** klicken, erscheint folgender Hinweis:

The following command will run SETUP quietly using Your transform file: setup.exe TRANSFORMS=U:\install\Office.XP\Standard.MST /qb-

Dieser Hinweis ist sehr wichtig für unser Vorhaben und wird direkt in die Routine **\\s1\netlogon\batch\InstallOfficeXP.cmd** zur automatischen Installation von Office XP eingehen.

Nachdem die gewünschten Voreinstellungen von Office mit dem Custom Installation Wizard getroffen und in einer MST-Datei fixiert wurden, erfolgt nun die automatische Installation von Office XP aus dem administrativen Installationspunkt **\\s1\install\office.xp**. Falls auf dem Windows XP-Computer bereits Office XP installiert ist, melden Sie sich als Administrator an und deinstallieren es über **Start · Einstellungen · Systemsteuerung · Software**. In diesem Fall löschen Sie auch über **Start · Einstellungen · Systemsteuerung · System · Erweitert** im mittleren Bereich **Benutzerprofile** über die Schaltfläche **Einstellungen** das Profil **TESTFIRMA\Testuser.** Ebenso löschen Sie ein eventuell auf dem Server in der Freigabe **Profiles** vorhandenes server-basiertes Anwenderprofil des Testusers. Wir wollen sichergehen, dass Office XP unter einem neuen Anwender ohne Vorlasten komplett neu installiert und genutzt werden kann, ohne dass Berechtigungsprobleme auftreten.

Um den Zweck dieser Übung, mehrere Anwendungen automatisch nacheinander zu installieren, ein wenig anschaulicher zu machen, deinstallieren Sie zusätzlich den in der vorangegangenen Übung installierten Acrobat Reader. Für den Testuser aktivieren wir jetzt in der Registerkarte die Batch-Routine **Offic-**

eXP.cmd und übernehmen vom Datenträger die beiden Routinen **OfficeXP.CMD** und **Batch\InstallOfficeXP.CMD**. Die Routine **\\s1\netlogon\OfficeXP.CMD** hat jetzt folgenden Inhalt:

```
@echo off
cls
echo Anmeldung an der Domaene %USERDNSDOMAIN%
net use u: /d > NUL: 2>&1
net use u: \\s1\install > NUL: 2>&1
c:
if not exist "c:\programme\Adobe\Acrobat 5.0\Reader\Acro-
Rd32.exe" %LOGONSERVER%\netlogon\util\intel.exe %LOGONSER-
VER%\netlogon\batch\InstallOfficeXP.cmd
```

Wenn also der Acrobat Reader noch nicht installiert ist, wird davon ausgegangen, dass es sich um eine »nackte« Windows XP-Installation handelt und alle benötigten Standardanwendungen nacheinander installiert werden sollen. Dazu wird mittels unseres SU-Tools **intel.exe** in einen User-Kontext mit lokalen administrativen Rechten gewechselt und die Unterroutine **netlogon\batch\InstallOfficeXP.cmd** gestartet. Diese installiert nacheinander mehrere Anwendungen, in unserem Beispiel zuerst den Acrobat Reader und danach das mittels des **Office Installation Wizard** vorkonfigurierte Office XP. Die Unterroutine **batch\InstallOfficeXP.cmd** hat folgenden Inhalt:

```
@echo off
cls
c:
net use u: /d > NUL: 2>&1
net use u: \\s1\install > NUL: 2>&1
echo Acrobat Reader wird installiert…
start /wait u:\AcrobatReader.505\setup -s
cls
echo Microsoft Office XP wird installiert…
u:\office.xp\setup.exe TRANSFORMS=u:\Office.XP\Standard.MST /qb-
```

Der Befehl **Start /wait** sorgt dafür, dass mit der Installation von Office XP gewartet wird, bis die Installation des Acrobat Readers komplett abgeschlossen ist. Die **setup.exe** von Office XP benötigt diesen Parameter übrigens nicht mehr, da das gewünschte Verhalten bereits in die **setup.exe** eingebaut ist. Bei der setup.exe von Office 2000 war das noch nicht so. Um sich über die Optionen des Start-Befehls zu informieren, geben Sie in einer DOS-Box den Befehl **Start /?** ein. Wenn Sie später das Installationsskript oder das Anmeldeskript

mit weiteren Routinen ausbauen, ist es wichtig, um die Möglichkeiten des Befehls **Start** und seiner Parameter zu wissen. Der Parameter **/MIN** ermöglicht z.B., einen im Hintergrund laufenden Prozess als minimiertes Fenster in die Taskleiste zu verbannen.

11.5 Der Microsoft Office XP Profile Wizard

Im Microsoft Office XP Resource Kit finden Sie das Tool **Microsoft Office XP Profile Wizard**. Mit diesem Tool können Sie alle Einstellungen, die unter einer bestimmten Kennung in Office XP vorgenommen wurden, in eine OPS-Datei schreiben. Diese Datei kann z.B. bei der Erstellung der MST-Datei mittels des Office Installation Wizard angegeben werden. Anwender, die sich später zum ersten Mal am System anmelden und Office XP starten, übernehmen dann diese Voreinstellungen. Die Verwendung des Profile Wizards ist aber nicht zwingend notwendig, da fast alle Office-Einstellungen auch über Gruppenrichtlinien von zentraler Stelle aus gesteuert werden können. Der Umgang mit dem Profile Wizard wird deshalb auch nur der Vollständigkeit halber in diesem Kapitel erklärt. Es kann jedoch für Sie in Spezialsituationen hilfreich sein, dieses Tool und die Möglichkeiten, die es bietet, zu kennen.

Der Profil Wizard des Microsoft Office XP Resource Kits muss auf dem Computer und unter der Kennung gestartet werden, von dem ein Mitschnitt des Office XP-Profils erstellt werden soll. Installieren Sie deshalb das Office XP Resource Kit temporär auf dem Mustercomputer. Sie können jedoch bei der Komponentenauswahl alle Tools bis auf den Office Profile Wizard abwählen.

Nutzen Sie eine neue Kennung wie z.B. **OfficeXP** (Vorname: Microsoft, Nachname: OfficeXP), die in der OU **Benutzer** eingerichtet wird. Es wird ein Exchange-Postfach erstellt, damit auch Outlook durchkonfiguriert werden kann. In der Registerkarte **Profil** der Kennung **OfficeXP** tragen Sie als Profilpfad **\\s1\profiles\OfficeXP** ein, Laufwerk **H:** verbinden Sie mit dem Home Directory **\\s1\userhome\OfficeXP**.

12.2 Die Windows XP-Vorlagedateien für Gruppenrichtlinien nutzen

Im Unterkapitel 16.6 »Die generelle Vorgehensweise zur Erstellung des Musterclients« des Kapitels 16 »Strategische Überlegungen und Tipps« können Sie nachlesen, über welches methodische Vorgehen man zu einem Verfahren gelangt, Abbilder von musterhaft installierten Computern zu erstellen, die dokumentiert, automatisiert und standardisiert sind und damit den Anforderungen eines Qualitätsmanagements gerecht werden. Nachdem durch die vorangegangenen Kapitel das Wissen zusammengetragen wurde, wie ein RIS-Server aufgesetzt und mit der RIS-Methode ein Computer mit Windows XP Professional eingerichtet wird, und nachdem Sie in dem Kapitel 10 über das Loginskript erfahren haben, mit welchen Tools Sie Installationsprozesse automatisieren können, soll dieses Kapitel nun Klarheit verschaffen, welche Einstellungen des Betriebssystems Windows XP Professional über Gruppenrichtlinien zentral verwaltet werden können. In den folgenden Kapiteln werden Sie dann erfahren, welche fehlenden Einstellungen Sie über selbst erstellte Gruppenrichtlinien vornehmen können, und wie Sie mit den Gruppenrichtlinien umgehen, die von Office XP/2003 zur Verfügung gestellt werden. Bevor dann das Abbild eines Mustercomputers gezogen werden kann, müssen jedoch weitere Vorarbeiten geleistet werden, die entweder automatisiert oder aufgrund einer Checkliste manuell vorgenommen werden.

Bei der Beschreibung der Gruppenrichtlinien werden auch die Schlüsselwerte genannt, die durch die Konfiguration dieser Richtlinien in der Registrierdatenbank geändert werden. Da Sie ein »Systemadministrator« und nicht nur ein »Mausadministrator« sind, sollte es Sie auch interessieren, welche Änderungen wo im Betriebssystem vorgenommen werden, wenn diese Gruppenrichtlinien konfiguriert werden.

Wenn Sie Windows XP Professional mit dem neuesten Service Pack installiert haben, finden Sie im Verzeichnis **C:\Windows\inf** sieben adm-Dateien. Es handelt sich um die Gruppenrichtlinien-Vorlagedateien von Windows XP. Kopieren Sie diese Dateien in das Unterverzeichnis **NETLOGON\adm** des Servers **S1**. Wie Sie in Kapitel 10 »Das Loginskript« gelesen haben, ist **NETLOGON** die Freigabe auf einem Domänencontroller, die Loginskripte aufnimmt.

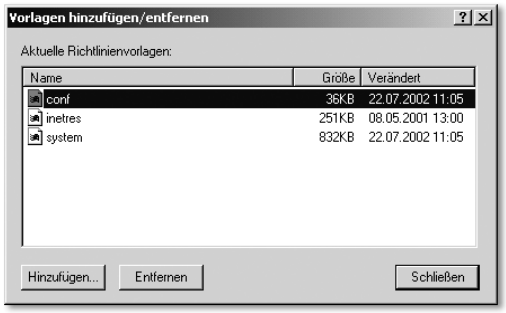
Um herauszufinden, welche Gruppenrichtlinien dieser Vorlagedateien genutzt werden sollten, richten Sie eine Organisationseinheit **Testfirma** unterhalb der Domäne **Testfirma.de** ein. Unterhalb der OU **Testfirma** richten Sie zwei weitere Sub-OUs mit den Bezeichnungen **Computer** und **Benutzer** ein. Verschieben Sie den Computer **MUSTERPC** aus dem Container **Computers** bzw. **RIS** in die neue Sub-OU **Computer** unterhalb der OU **Testfirma**.

Erstellen Sie in der Sub-OU **Benutzer** eine neue Kennung **Testuser** mit dem vollen Namen **Hugo Testuser**. Wenn diese Kennung bereits existiert, weil Sie sie bereits beim Durcharbeiten des Kapitels »Das Loginskript« benutzt haben, so löschen Sie zuerst sowohl die Kennung als auch ein eventuell vorhandenes Userhome Directory und Profile Directory, um ohne Vorlasten zu testen.

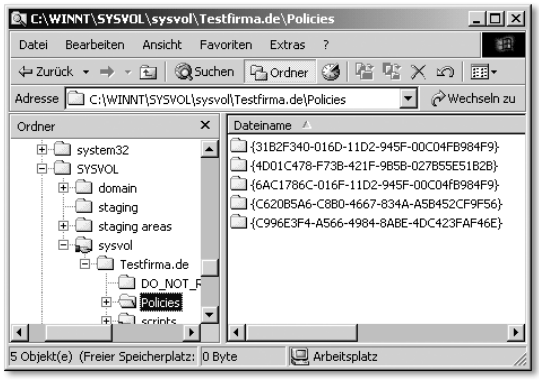
Richten Sie nun eine neue XP-Gruppenrichtlinie für die Sub-OU **Computer** ein: Öffnen Sie die Eigenschaften der Sub-OU, dort die Registerkarte **Gruppenrichtlinien** und starten Sie die Schaltfläche **Neu**. Als Name für die neue Gruppenrichtlinie wählen Sie **XP-Standardcomputer**, weil diese Richtlinie für den Standardcomputer gelten soll.

Wählen Sie die Schaltfläche **Eigenschaften** und aktivieren Sie die Option **Benutzerdefinierte Konfigurationseinstellungen deaktivieren**. Da diese Gruppenrichtlinie nur auf den Schlüssel **HKEY_LOCAL_MACHINE** der Registrierdatenbank angewendet wird, führt die Deaktivierung der benutzerdefinierten Konfigurationseinstellungen dazu, dass die Gruppenrichtlinie schneller abgearbeitet wird.

Wählen Sie **OK** und danach **Bearbeiten**. Wählen Sie unter **Computerkonfiguration** die **Administrativen Vorlagen** mit der rechten Maustaste an und klicken Sie auf **Vorlagedateien hinzufügen/entfernen**. Im neuen Fenster **Vorlagen hinzufügen/entfernen** sehen Sie die Standardvorlagedateien, die beim Erstellen einer neuen Gruppenrichtlinie geladen werden. Es handelt sich um die Dateien **conf.adm**, **inetres.adm** und **system.adm**.



Beim Erstellen einer neuen Gruppenrichtlinie wird im Verzeichnis **C:\Winnt\SYSVOL\sys-vol\Testfirma.de\Policies** ein Unterverzeichnis generiert, dessen Name eine kryptische Aneinanderreihung von Buchstaben und Zahlen, eingeschlossen in geschweiften Klammern, ist.



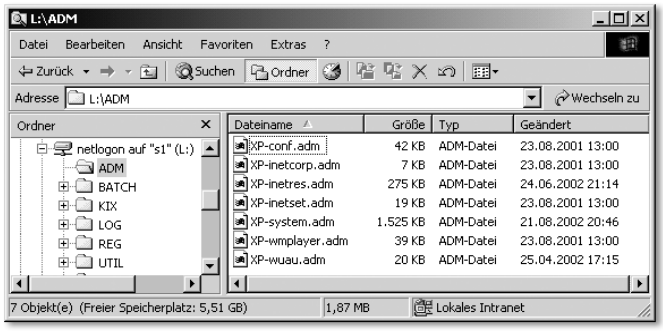
Wenn Sie die Eigenschaften der Gruppenrichtlinie aufrufen, finden Sie diesen Verzeichnisnamen in der Registerkarte **Allgemein** im Feld **Eindeutiger Name**.

Unterhalb dieses Verzeichnisses werden die Unterverzeichnisse **ADM**, **Machine** und **User** automatisch erzeugt und die Dateien **conf.adm**, **inetres.adm** und **system.adm** aus dem Verzeichnis **%SYSTEMROOT%\inf** in das generierte Verzeichnis **ADM** kopiert. Arbeiten Sie mit Windows 2000 Server, so handelt es sich um Vorlagedateien für Windows 2000 Server bzw. für Windows 2000 Professional. Arbeiten Sie mit Windows Server 2003, so sind diese Vorlagedateien bereits für Windows XP erweitert.

Wenn Sie unter Windows 2000 Server die Vorlagedateien von Windows XP verwenden wollen, müssen Sie im Fenster **Vorlagen hinzufügen/entfernen** die drei Vorlagen **conf**, **inetres** und **system** zuerst über die Schaltfläche **Entfer-**

nen entladen und dann über die Schaltfläche **Hinzufügen** die gewünschten XP-Vorlagen laden.

Ein Tipp unter Windows 2000 Server: Da die Vorlagedateien von Windows XP dieselben Namen haben wie die Vorlagedateien von Windows 2000, können Sie später in einer komplexeren Umgebung nicht mehr unterscheiden, ob in einer bestimmten Gruppenrichtlinie die Vorlagedateien von Windows 2000 oder von Windows XP geladen wurden. Ich schlage Ihnen deshalb vor, zuerst alle von Windows XP übernommenen Dateien ***.adm** in **XP-*.adm** umzubenennen und dann diese XP-*.adm-Vorlagedateien hinzuzufügen.



Da Sie später die Windows XP-Gruppenrichtlinien-Vorlagedateien und auch selbst erstellte ADM-Vorlagedateien noch oft hinzuladen werden, bietet es sich an, die in **XP-xyz.adm** umbenannten Vorlagedateien von Windows XP in das Verzeichnis **%SYSTEMROOT%\inf** des Servers zu kopieren, denn dann werden diese Vorlagedateien wie die original Windows 2000-Vorlagedateien sofort angezeigt, sobald Sie die Schaltfläche **Hinzufügen** im Fenster **Vorlagen hinzufügen/entfernen** anklicken. Alternativ könnten Sie auch die gleichnamigen Dateien im Verzeichnis **%SYSTEMROOT%\inf** des Servers überschreiben. Denn die für Windows XP erweiterten adm-Dateien sind bezüglich Windows 2000 Professional abwärts kompatibel. Abwärtskompatibilität bedeutet in diesem Fall, dass die Vorlagedateien von Windows XP auch in einer Mischumgebung von Clients mit Windows 2000 Professional und Windows XP verwendet werden können. Die Erweiterungen dieser adm-Dateien um Richtlinien speziell für Windows XP werden von Windows 2000 Professional-Clients ignoriert. Sollte jedoch später einmal ein neues Service Pack zu Windows 2000 Server eingespielt werden, so müssen Sie sicherstellen, dass die bezüglich Windows XP erweiterten adm-Dateien beim Einspielen dieses Service Packs nicht durch

adm-Dateien überschrieben werden, bei denen die Erweiterungen für Windows XP fehlen. Verlassen Sie sich nicht darauf, dass Microsoft bei der Veröffentlichung des nächsten Service Packs für Windows 2000 Server dieses Problem einbezieht!

Wenn Sie mit Windows Server 2003 arbeiten, müssen Sie sich um diese Dinge keine Gedanken mehr machen, denn die Vorlagedateien von Windows Server 2003 sind weitgehend identisch mit denen von Windows XP.

Wichtiger Hinweis: Gruppenrichtlinien-Vorlagedateien (*.adm-Datei) erweitern nur die Kategorie **Administrative Vorlagen**. Diese Kategorie finden Sie sowohl unter **Computerkonfiguration** als auch unter **Benutzerkonfiguration**, wenn Sie eine Gruppenrichtlinie über die Schaltfläche **Bearbeiten** öffnen. Wenn Sie eine *.adm-Datei hinzufügen, werden jedoch die neuen Richtlinien nicht immer sofort angezeigt. Um sicher zu sein, dass Sie alle Richtlinien anschließend in beiden Kategorien **Computerkonfiguration** als auch **Benutzerkonfiguration** sehen, schließen Sie nach dem Hinzuladen einer adm-Datei die Gruppenrichtlinie und öffnen Sie sie erneut über die Schaltfläche **Bearbeiten**.

Doch welche der XP-Gruppenrichtlinien-Vorlagedateien sollen geladen werden? Welche Funktion haben die verschiedenen *.adm-Dateien? Sie können alle Windows XP-ADM-Dateien mit **Notepad.exe** ansehen und bearbeiten. Sie können auch alle Windows XP-ADM-Dateien einzeln nacheinander laden, um zu sehen, welche Änderungen sich jeweils unter **Computerkonfiguration** und unter **Benutzerkonfiguration** ergeben. Dabei stellen Sie Folgendes fest:

- **XP-conf.adm** ist für Netmeeting-Richtlinien zuständig und stellt Richtlinien unter **Computerkonfiguration** und unter **Benutzerkonfiguration** zur Verfügung.
- **XP-inetcorp.adm** stellt unter **Benutzerkonfiguration** eine Richtlinie für die Wartung des Internet Explorers zur Verfügung, die sich aber nicht starten lässt.
- **XP-inetres.adm** ist ebenfalls für den Zugriff auf das Internet zuständig und stellt hierfür sowohl unter **Computerkonfiguration** als auch unter **Benutzerkonfiguration** Richtlinien bereit.
- **XP-system.adm** stellt sowohl unter **Computerkonfiguration** als auch unter **Benutzerkonfiguration** viele wichtige Richtlinien bereit.

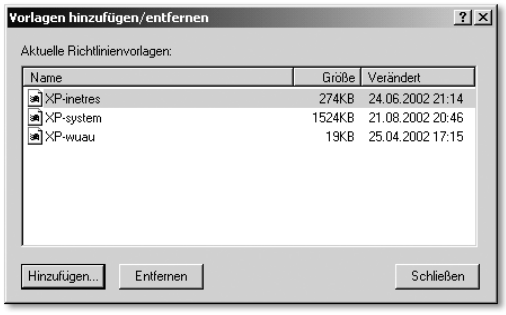
- **XP-wmplayer** enthält nur benutzerbezogene Gruppenrichtlinieneinstellungen für den Windows Media Player.
- **XP-wuau.adm** enthält nur maschinenbezogene Gruppenrichtlinieen für den Windows Update Service.

Solange Sie Netmeeting nicht einsetzen, sollten Sie die Gruppenrichtliniendatei **XP-conf.adm** nicht hinzuladen. Für die gerade in der OU **Computer** erstellte Gruppenrichtlinie **XP-Standardcomputer** sind die Richtliniedateien **XP-inetres.adm**, **XP-system.adm**, **XP-wuau.adm** interessant.

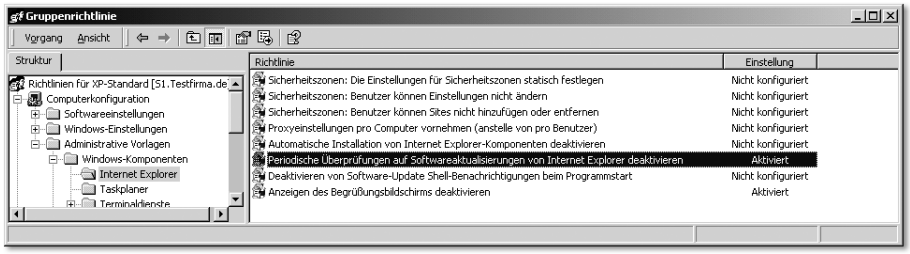
In der OU **Benutzer** werden wir später ebenfalls eine Gruppenrichtlinie mit dem Namen XP-Standardbenutzer erstellen. Für diese Gruppenrichtlinie werden dann die Gruppenrichtliniendateien **XP-inetres.adm**, **XP-system.adm** und **XP-wmplayer.adm** geladen.

12.3 Festlegen der Gruppenrichtlinien für den Standard-Computer

Wählen Sie nun die Eigenschaften der Gruppenrichtlinie **XP-Standardcomputer** in der OU **Computer** an, klicken Sie auf **Bearbeiten**, wählen Sie unter **Computerkonfiguration** die **Administrativen Vorlagen** mit der rechten Maustaste an und klicken Sie auf **Vorlagedateien hinzufügen/ entfernen**. Wenn Sie mit Windows 2000 Server statt mit Windows Server 2003 arbeiten, entfernen Sie im neuen Fenster **Vorlagen hinzufügen/entfernen** zuerst die Windows 2000-Vorlagen **conf**, **inetres** und **system**. Danach fügen Sie die Windows XP-Vorlagen **XP-inetres.adm**, **XP-system.adm** und **XP-wuau.adm** hinzu.



Jetzt werden alle Richtlinien in der Kategorie **Computerkonfiguration** durchgesehen und wichtige Richtlinien aktiviert bzw. konfiguriert.



Die Aktivierung der Richtlinie **Periodische Überprüfungen auf Softwareaktualisierungen von Internet Explorer deaktivieren** deaktiviert die Überprüfung, ob eine neue Version des Browsers verfügbar ist. Es werden die Überprüfung, ob die aktuellste verfügbare Browserversion installiert ist, und die Benachrichtigung über eine verfügbare neue Version deaktiviert, wenn Sie diese Richtlinie aktivieren. Ohne Aktivierung dieser Richtlinie wird standardmäßig im Abstand von 30 Tagen überprüft, ob eine neue Version verfügbar ist.

Die Aktivierung der Richtlinie **Anzeigen des Begrüßungsbildschirms beim Programmstart** deaktiviert die Anzeige des Internet Explorer-Begrüßungsbildschirms beim Browserstart. Der Begrüßungsbildschirm, der Programmnamen, Lizenz- und Copyright-Informationen enthält, wird nicht angezeigt, wenn Sie diese Richtlinie aktivieren.

In der Kategorie **Windows Installer** können Sie die Erstellung von Systemwiederherstellungsprüfpunkten deaktivieren, wodurch ein einfacher Benutzer keine neuen Systemwiederherstellungspunkte über **Start · Programme · Zubehör · Systemprogramme · Systemwiederherstellung** mehr erzeugen kann.

Mit der Systemwiederherstellung können Benutzer im Falle eines Problems ihre Computer in einem früheren Zustand wiederherstellen, ohne dass persönliche Datendateien verloren gehen. Standardmäßig erstellt Windows Installer bei jeder Installation einer Anwendung automatisch einen Systemwiederherstellungsprüfpunkt. Dadurch können Benutzer ihren Computer in den Zustand

wiederherstellen, den er vor der Installation der Anwendung aufwies. Durch die Aktivierung der Richtlinie **Erstellung von Systemwiederherstellungsprüfpunkten deaktivieren** kann nur noch ein Administrator über **Start · Programme · Zubehör · Systemprogramme · Systemwiederherstellung** einen neuen Prüfpunkt erstellen. Jeder andere Anwender erhält bei dem Versuch folgende Fehlermeldung:

Beachten Sie bitte, dass es zwei weitere Richtlinien in der Kategorie **Computerkonfiguration · Administrative Vorlagen · System –Systemwiederherstellung** gibt:

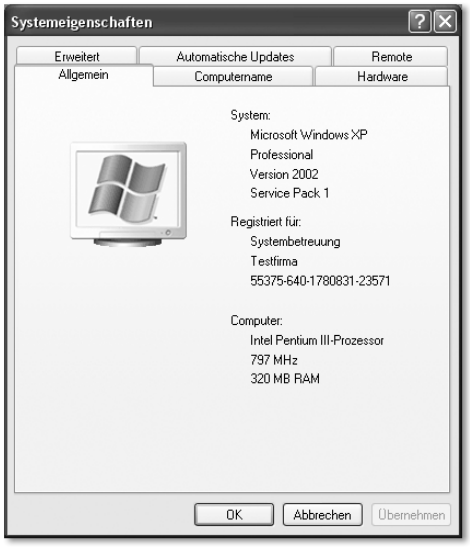
Systemwiederherstellung deaktivieren und **Konfiguration deaktivieren**.

Die Richtlinie **Systemwiederherstellung deaktivieren** legt fest, ob die Systemwiederherstellung ein- oder ausgeschaltet ist. Die Systemwiederherstellung ermöglicht es dem Benutzer bei Vorliegen eines Problems den Computer auf einen vorherigen Zustand zurückzusetzen. Standardmäßig ist die Systemwiederherstellung eingeschaltet. Wenn der Administrator auf einem Windows XP-Computer über die Systemsteuerung das Icon **System** starten und dann die Registerkarte **Systemwiederherstellung** anwählt, stellt er fest, dass per Standardeinstellung der Maximalwert für Systemwiederherstellungsprüfpunkte 12 % der Systempartition beträgt.

In der Registrierdatenbank finden Sie unter **KHEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\SystemRestore** den Schlüssel **DiskPercent**. Bei aktivierter Systemwiederherstellung hat er den Wert **12**, bei deaktivierter **Systemwiederherstellung** den Wert **c**. Hier finden Sie auch den Schlüssel **DisableSR**, der bei Deaktivierung von **0** auf **1** umgestellt wird. Wird eine der Richtlinien **Systemwiederherstellung deaktivieren** und **Konfiguration deaktivieren** eingestellt, so finden Sie nach dem nächsten Start des Windows XP-Computers unter **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\SystemRestore** die Schlüssel **DisableRestore** und **DisableConfig** mit entsprechenden Werten.

Die Aktivierung der Richtlinie **Erstellung von Systemwiederherstellungsprüfpunkten deaktivieren** erzeugt unter **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer** den Schlüssel **LimitSystemRestoreCheckpointing**.

Durch Aktivierung der Richtlinie **Systemwiederherstellung deaktivieren** wird auch für den Administrator unter **Systemsteuerung · System** die Registerkarte **Systemwiederherstellung** komplett ausgeblendet.

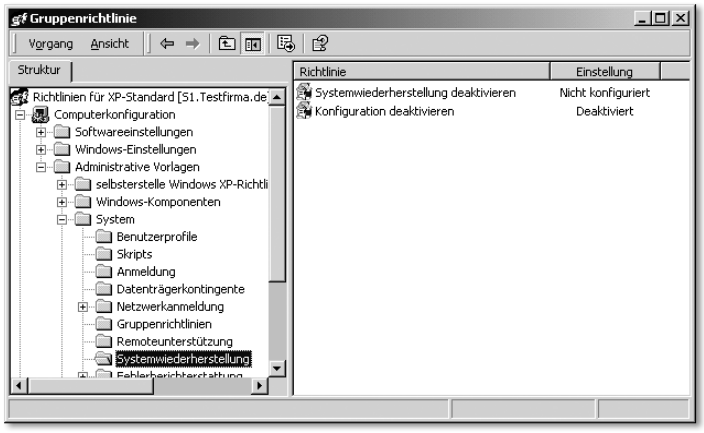


Die Beschreibung der zweiten Richtlinie **Konfiguration deaktivieren** ist ein wenig verwirrend:

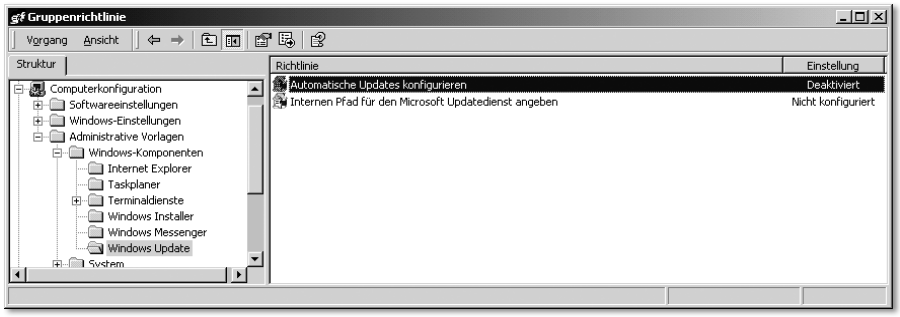
> *»Die Systemwiederherstellung ermöglicht es dem Benutzer bei Vorliegen eines Problems den Computer auf einen vorherigen Zustand zurückzusetzen, ohne persönliche Dateien zu verlieren. Das Verhalten dieser Einstellung ist abhängig von der Einstellung von »Systemwiederherstellung deaktivieren«.*

Wenn Sie diese Einstellung aktivieren, verschwindet die Möglichkeit, die Systemwiederherstellung auf der Konfigurationsschnittstelle zu konfigurieren. Wenn die Einstellung »Konfigurationseinstellung deaktivieren« deaktiviert ist, ist die Konfigurationsschnittstelle noch sichtbar, es werden jedoch alle Standardwerte der Systemwiederherstellungskonfiguration erzwungen. Wenn Sie sie nicht konfigurieren, bleibt die Konfigurationsschnittstelle für die Systemwiederherstellung, und der Benutzer kann die Systemwiederherstellung konfigurieren.«

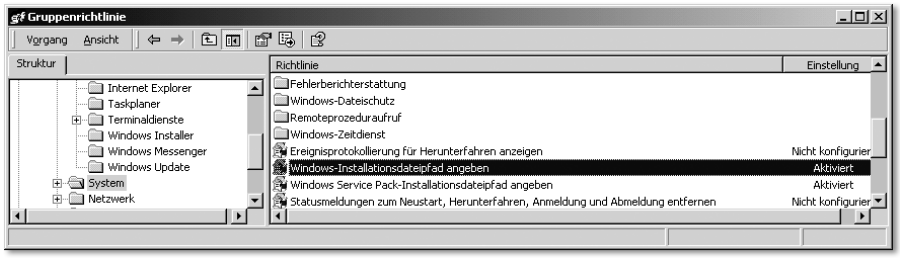
Gemeint ist Folgendes: Wenn die Richtlinie **Systemwiederherstellung deaktivieren** nicht konfiguriert ist, und die Richtlinie **Konfiguration deaktivieren** deaktiviert ist, kann der Administrator die Registerkarte **Systemwiederherstellung** zwar über **Systemsteuerung · System** aufrufen, sieht darin, dass die Systemwiederherstellung über eine Gruppenrichtlinie deaktiviert wurde, kann aber diese Einstellung nicht verändern. Ein einfacher Benutzer sieht auch weiterhin nicht die Registerkarte **Systemwiederherstellung**.



Da Sie in Ihrer Organisation nur durchgetestete und mit Ihrer Umgebung kompatible Anwendungen einsetzen werden, und der einfache Anwender keine weiteren Anwendungen oder Hardwaretreiber installieren darf, können Sie wahrscheinlich auf das Windows XP Feature **Systemwiederherstellung** verzichten, auf jeden Fall aber unterbinden, dass der Standardanwender neue Systemwiederherstellungspunkte erstellen darf. Die Systemwiederherstellungspunkte speichern auf der lokalen Festplatte den Zustand des Systems vor der Installation einer neuen Anwendung. Dadurch geht Speicherplatz verloren. Da Sie noch einige Standardanwendungen wie Microsoft Office, den Acrobat Reader und vielleicht eine kaufmännische Anwendung wie z.B. den SAP-Client installieren werden, bevor Sie ein Abbild (Image) ziehen, können Sie zumindest für diese vorher durchgetesteten Anwendungen die Erstellung von Systemwiederherstellungspunkten deaktivieren.

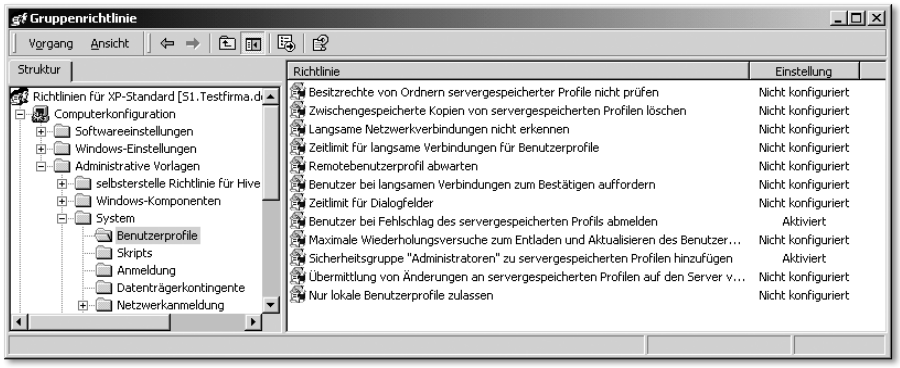


Falls die Richtlinie **Automatische Updates konfigurieren** deaktiviert ist, müssen alle verfügbaren Updates vom Administrator auf der Windows Update Website (http://windowsup-date.microsoft.com) manuell heruntergeladen, getestet und zur Installation freigegeben werden. Die Clients versuchen also nicht, selbstständig und ohne Ihre Kontrolle Updates zu installieren.

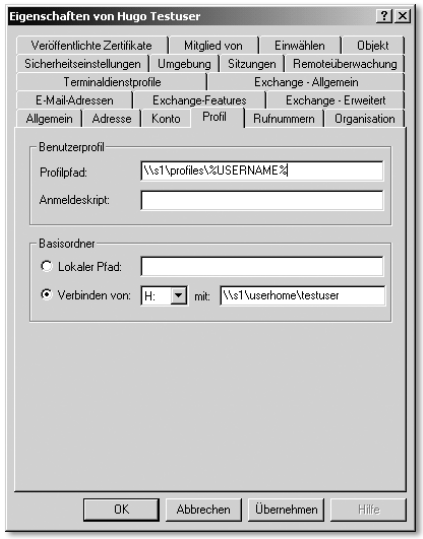


Über die Aktivierung der Richtlinien **Windows-Installationsdateipfad angeben** und **Windows Service Pack-Installationsdateipfad angeben** können Sie erreichen, dass die Quelldateien von nachzuinstallierenden Komponenten im Verzeichnis **Install\WindowsXP** des Servers gesucht werden, statt vom CD-ROM-Laufwerk bzw. aus der Freigabe **RemoteInstall** eines Servers, von dem ursprünglich mittels RIS der Client aufgesetzt wurde. In Kapitel 10 »Das Loginskript« wurde gesagt, dass es sinnvoll ist, für alle Anwender im Loginskript das Laufwerk **U:** oder ein anderes, fest für diesen Zweck definiertes Laufwerk über den Befehl **net use u: \\Servername\Install** mit dem Software-Archiv des Servers am jeweiligen Standort zu verbinden. Wenn Sie diese beiden Richtlinien aktivieren und als Pfad jeweils **U:\WindowsXP** eintragen, können Komponenten von Windows XP jederzeit nachinstalliert werden, vorausgesetzt, der angemeldete Anwender hat die Berechtigungen zur Installation von Komponenten.

In der Kategorie **Computerkonfiguration · Administrative Vorlagen · System · Benutzerprofile** sollten Sie auf jeden Fall die Richtlinie **Sicherheitsgruppe »Administratoren« zu server-gespeicherten Profilen hinzufügen** aktivieren.



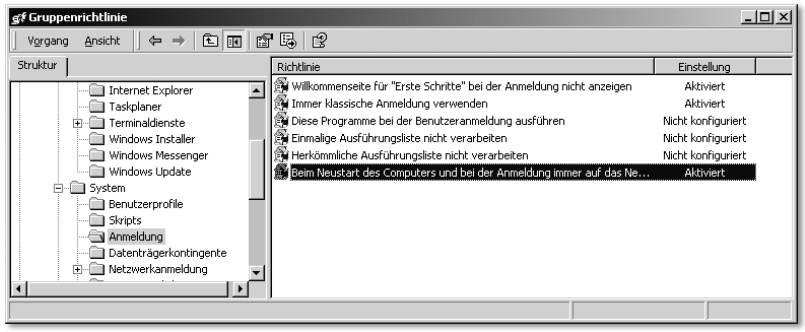
Der Hintergrund ist Folgender: Wenn Sie auf dem Server ein Verzeichnis mit dem Namen **Profiles** anlegen und unter demselben Namen freigeben, so können Sie für bestimmte Anwender so genannte server-gespeicherte Benutzerprofile (Roaming Profiles) anlegen. Wenn Sie anschließend für die Kennung **Testuser** in der Registerkarte **Profil** als Profilpfad **\\s1\profiles\%USERNAME%** eintragen, wird bei der nächsten Anmeldung des Anwenders Testuser automatisch unterhalb der Freigabe **Profiles** ein Verzeichnis mit der Anmeldekennung des sich anmeldenden Anwenders erzeugt und das Profil der Kennung von **C:\Dokumente und Einstellungen\Testuser** dorthin kopiert. Jedoch erhält nur das System und der Anwender Testuser selbst Vollzugriff auf das generierte Profilverzeichnis **\\s1\profiles\Testuser**, der Administrator kann es nicht einmal einsehen. Durch die Aktivierung der Richtlinie **Sicherheitsgruppe »Administratoren« zu server-gespeicherten Profilen hinzufügen** erhält auch der Administrator Vollzugriff auf neu erstelle Profilverzeichnisse des Servers. Ohne dieses Recht ist der Administrator z.B. nicht befugt, dieses Serververzeichnis zu löschen, wenn die Kennung **Testuser** nicht mehr benötigt wird, und damit auch das server-gespeicherte Benutzerprofil gelöscht werden soll.



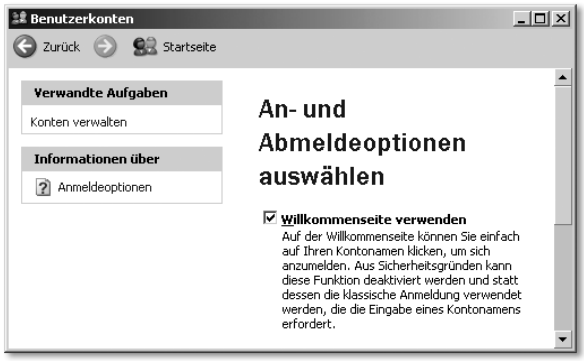
Durch Aktivierung der Richtlinie **Benutzer bei Fehlschlag des server-gespeicherten Profils abmelden** können Sie verhindern, dass ein Benutzer sich mit der unter **C:\Dokumente und Einstellungen** vorhandenen lokalen Kopie des server-gespeicherten Profils auch dann lokal anmelden kann, wenn kein Anmeldeserver antwortet bzw. der Server mit dem server-gespeicherten Profil nicht antwortet.

Diese Richtlinie sollten Sie nicht für Laptops aktivieren, denn Laptop-Besitzer sollen sich ja gerade auch dann anmelden können, wenn ihr Laptop nicht mit dem Netzwerk verbunden ist!

Das Aktivieren der Richtlinie **Willkommenseite für »Erste Schritte« bei der Anmeldung nicht anzeigen** blendet die Willkommenseite aus, die bei jeder Benutzeranmeldung auf Windows 2000 Professional und Windows XP Professional angezeigt wird.



Durch das Aktivieren der Richtlinie **Immer klassische Anmeldung verwenden** wird der Benutzer gezwungen, sich mit dem klassischen Anmeldebildschirm am Computer anzumelden. Dieser Anmeldebildschirm hat das alte Design von Windows 2000 Server. Bei einem Windows XP-Computer, der nicht an eine Domäne angebunden ist, werden im Anmeldebildschirm standardmäßig die lokal eingerichteten Benutzerkennungen angezeigt. Über **Systemsteuerung · Benutzerkonten · Art der Benutzeranmeldung ändern** können Sie aber auch unter Windows XP die Option **Willkommenseite verwenden** deaktivieren und den klassischen Anmeldeschirm erzwingen, der die Eingabe eines Kontonamens erfordert. Bei Windows XP-Clients, die Mitglieder einer Domäne sind, wird immer der klassische Anmeldeschirm angezeigt.

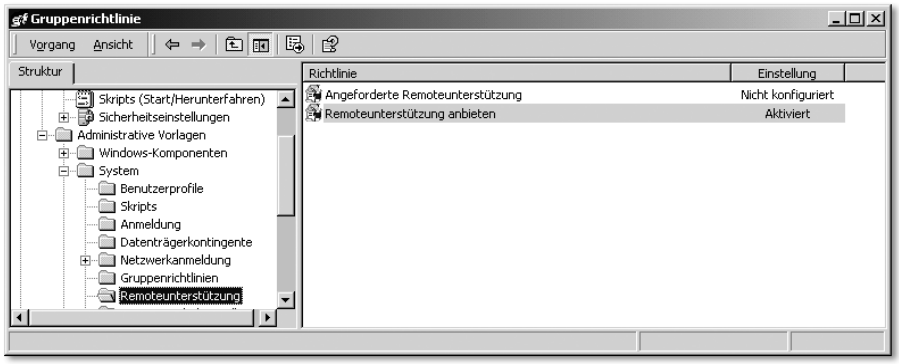


Die Aktivierung der Richtlinie **Beim Neustart des Computers und bei der Anmeldung immer auf das Netzwerk warten** wird in der Erklärung zur Richtlinie wie weiter unten stehend beschrieben und sollte deshalb aktiviert werden:

> *»Legt fest, ob Windows XP beim Start des Computers und bei der Benutzeranmeldung auf das Netzwerk wartet. Standardmäßig wartet Windows XP beim Start und bei der Benutzeranmeldung nicht, bis das Netzwerk vollständig konfiguriert ist. Vorhandene Benutzer werden angemeldet, indem zwischengespeicherte Zugangsberechtigungen verwendet werden, was zu kürzeren Anmeldezeiten führt. Wenn das Netzwerk verfügbar wird, werden im Hintergrund Gruppenrichtlinien angewendet.*
>
> *Man beachte, dass dies eine Aktualisierung im Hintergrund ist, Erweiterungen wie Softwareinstallation und Ordnerumleitung zwei Anmeldungen benötigen, damit die Änderungen wirksam werden. Um sicher arbeiten zu können, erfordern diese Erweiterungen, dass keine Benutzer angemeldet sind. Daher müssen sie im Vordergrund bearbeitet werden, bevor Benutzer den Computer aktiv verwenden. Zusätzlich dazu kann es sein, dass für Änderungen am Benutzerobjekt, wie z.B.*

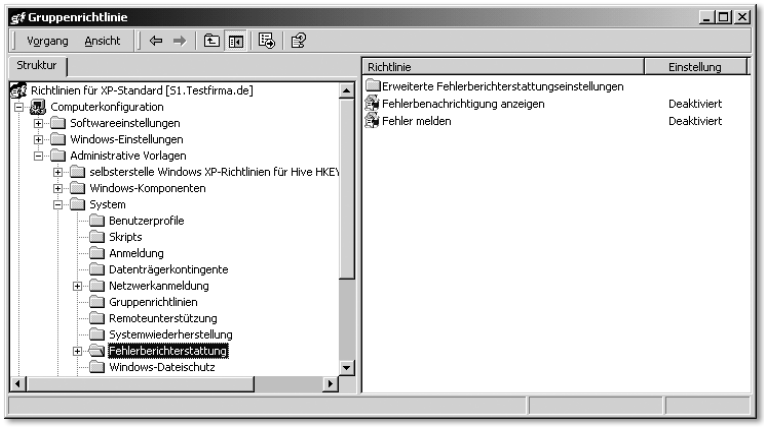
Hinzufügen eines Pfades eines server-gespeicherten Profils, eines Basisverzeichnisses oder eines Benutzerobjekt-Anmeldeskripts das Erkennen von bis zu zwei Anmeldungen erforderlich ist. ...

Hinweis: Wenn Sie die Anwendung der Ordnerumleitung, Softwareinstallation oder der Einstellungen von server-gespeicherten Profilen in nur einem Anmeldevorgang garantieren wollen, aktivieren Sie diese Einstellung, um sicherzustellen, dass Windows darauf wartet, dass das Netzwerk zur Verfügung steht, bevor die Richtlinien angewendet werden.«



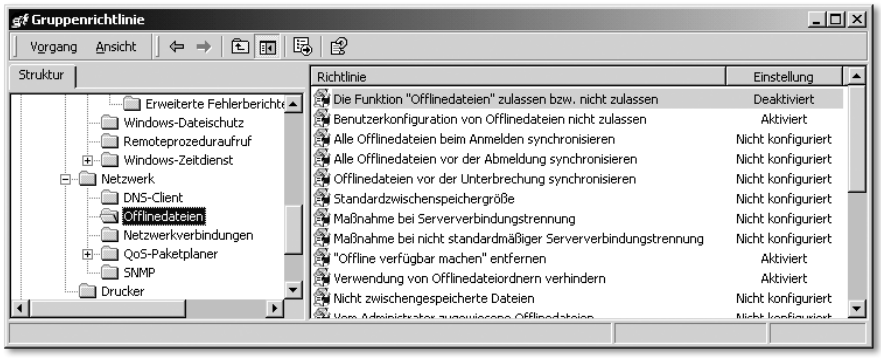
Über die Aktivierung der Richtlinie **Remoteunterstützung anbieten** können Sie einzelne Mitarbeiter oder eine Gruppe von Mitarbeitern angeben, die die Steuerung eines anderen PCs übernehmen darf (Fernwartung), um vom eigenen Arbeitsplatz aus einem Mitarbeiter Hilfe anzubieten.

Wenn die Richtlinien **Fehlerbenachrichtigung anzeigen** und **Fehler melden** deaktiviert sind, werden Meldungen über Programmfehler nicht an Microsoft gesendet.



Durch die verschiedenen Richtlinien unter **Offlinedateien** können Sie verhindern, dass sensible Unternehmensdaten durch die Offline-Synchronisation auf lokale Festplatten geraten. Wenn in Ihrem Unternehmen alle Daten nur auf den Servern liegen sollen und es keine Mitarbeiter gibt, die mit Laptops arbeiten bzw. Dokumente offline zuhause oder beim Kunden im Zugriff haben sollen, so können Sie über diese Richtlinien bereits in der Computerkonfiguration verhindern, dass Daten zwischen dem Server und dem Client synchronisiert werden oder der Anwender an den Einstellungen der Offline-Synchronisation manipulieren kann.

Sie können dieselben Einstellungen auch unter **Benutzerkonfiguration** vornehmen. Wenn es also eine Sicherheitsgruppe gibt, die offline mit Firmendaten arbeiten können muss, so sollten Sie diese Einstellungen nicht unter **Computerkonfiguration** vornehmen, sondern spezielle Offline-Gruppenrichtlinien für bestimmte Anwendergruppen erstellen und die Richtlinien in der **Benutzerkonfiguration** vornehmen. Alternativ kann eine spezielle OU für Laptops eingerichtet werden, in der eine Gruppenrichtlinie für Offlinedateien konfiguriert wird.

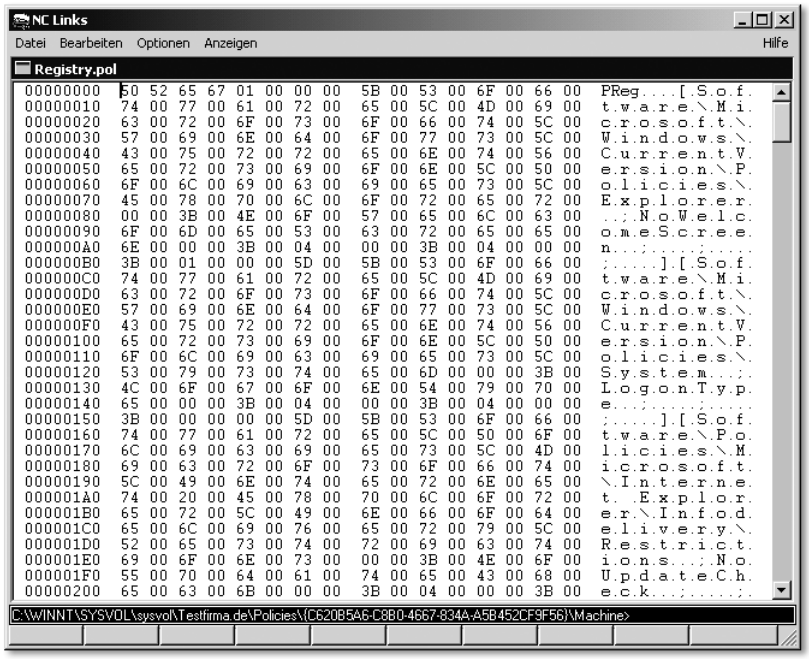


Ein wichtiger Hinweis: Einstellungen unter **Computerkonfiguration** überschreiben in der Regel gleichnamige Einstellungen unter **Benutzerkonfiguration**!

12.3.1 Wo werden die Einstellungen im Bereich »Computerkonfiguration« auf dem Domänencontroller gespeichert?

Sie haben nun über das Snap-In **Active Directory-Benutzer und -Computer** Änderungen an einer Gruppenrichtlinie im Bereich **Computerkonfiguration** vorgenommen, und diese Änderungen werden in der Registrierdatenbank jedes Clients vorgenommen, der sich in der OU **Computer** unterhalb der OU

Testfirma befindet. Wo auf dem Server werden aber diese Änderungen abgespeichert? Im Verzeichnis **C:\WINNT\SYSVOL\sysvol\Testfirma.de\Policies\{Eindeutiger Name der Gruppenrichtlinie}\Machine** finden Sie jetzt eine Datei namens **Registry.pol**. Wenn Sie die Datei **Registry.pol** mit einem Hex-Editor öffnen, sehen Sie Folgendes:



In der rechten Spalte können Sie lesen, in welchen Pfaden der Registry Änderungen vorgenommen werden, unter **HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Policies** und unter **HKEY_LOCAL_MACHINE/Software/Policies**. Da die gesamte Gruppenrichtlinie unterhalb von **C:\WINNT\SYSVOL** gespeichert wird und da das gesamte Verzeichnis **C:\WINNT\SYSVOL** zwischen allen Domänencontrollern der Domäne repliziert wird, muss ein Client-Computer, der in einem anderen Standort steht, nicht bei jedem Start die Gruppenrichtlinie über die langsame WAN-Verbindung vom Server auslesen, auf dem die Gruppenrichtlinie erstellt wird. Der Client in einer Filiale meldet sich an einem Domänencontroller in der Filiale an und liest die auf diesem Domänencontroller replizierte Gruppenrichtlinie aus. Das verringert die Netzlast und führt zu einer besseren Verfügbarkeit des gesamten Netzwerks, wenn irgendwo in der Organisation einmal ein Domänencontroller ausfällt oder gewartet werden muss und somit nicht verfügbar ist.

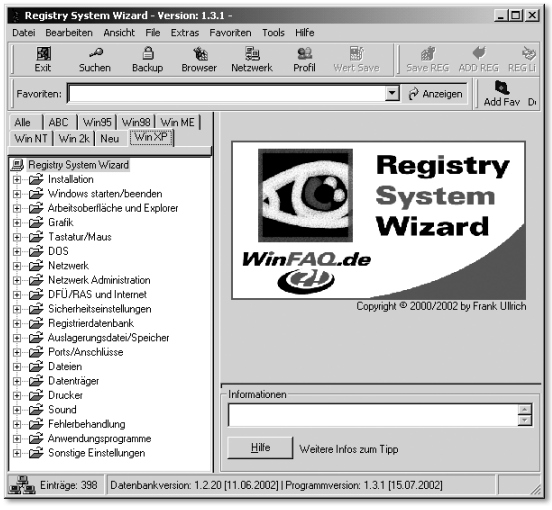
13 Vorlagedateien für fehlende Gruppenrichtlinien selbst erstellen

Da Sie über Gruppenrichtlinien viele Einstellungen des Client-Betriebssystems und der auf dem Client laufenden Anwendungen von zentraler Stelle aus steuern können, liegt es nahe, für alle Registrierdatenbankeinträge selber Gruppenrichtliniendateien zu erstellen, wenn der Hersteller keine ADM-Dateien oder passenden Gruppenrichtlinien anbieten kann.

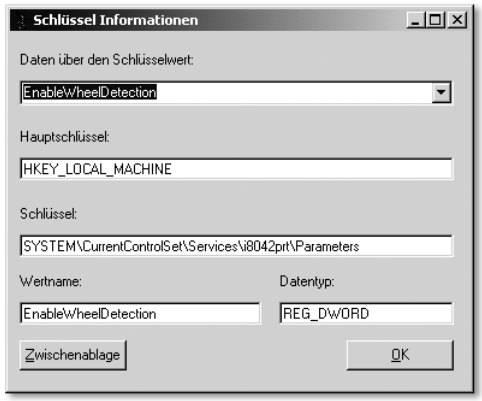
13.1 Vorlagedateien mit dem Tool »Registry System Wizard« erstellen

Über Gruppenrichtlinien können nur die Zweige **HKEY_CURRENT_USER** und **HKEY_LOCAL_MACHINE** der Registrierdatenbank verändert werden, nicht aber Einträge **HKEY_CLASSES_ROOT, HKEY_USERS, HKEY_CURRENT_CONFIG**.

Das Erstellen einer eigenen ADM-Datei ist nicht so kompliziert, wie man vielleicht vermuten wird. Besonders hilfreich kann hier ein Tool wie **Registry System Wizard** sein, das Sie über www.winfaq.de bzw. über www.wintotal.de beziehen können. Nach dem Start von **Registry System Wizard** wählen Sie über eine Registerkarte das Betriebssystem **Windows XP** oder **Windows 2000** aus, für das Sie Änderungen an der Registrierdatenbank vornehmen wollen. Danach werden nach Kategorien geordnet alle möglichen Tipps aufgelistet, mit denen Sie die Registrierdatenbank Ihren Wünschen entsprechend verändern können.



Wenn Sie z. B. wissen möchten, welche Änderung an der Registrierdatenbank vorgenommen werden muss, um nachträglich eine Maus mit Rad zu aktivieren, wechseln Sie in die Kategorie **Tastatur/Maus**. Dort finden Sie den entsprechenden Tipp und nach Betätigung der Schaltfläche **KeyInfo** den Registry-Wert, der verändert werden muss.



Sie können nun den Registry System Wizard auf einem Computer mit Windows XP Professional installieren und anschließend nach interessanten Einstellmöglichkeiten suchen, für die die von Microsoft zur Verfügung gestellten Windows XP-Gruppenrichtliniendateien keine Richtlinien anbieten.

Wenn Sie im Registry System Wizard den Menüpunkt **File** aufrufen, stellen Sie fest, dass Sie eine REG-Datei bzw. eine ADM-Datei erstellen können und danach weitere Einstellungen über die Befehle **Tipp zur REG-File Liste hinzufügen** bzw. **Tipp zur ADM-File Liste hinzufügen** der erzeugten Datei hinzufügen können. Der Menüpunkt **ADM-File vom aktuellen Tipp erstellen** bzw. der Menüpunkt **Tipp zur ADM-File Liste hinzufügen** steht jedoch nicht bei allen Tipps zur Verfügung. Das liegt unter anderem daran, dass mit einer Richtliniendatei (*.adm-Datei) nur die Zweige **HKEY_LOCAL_MACHINE und HKEY_CURRENT_USER** manipuliert werden können, nicht aber die drei anderen Zweige **HKEY_CLASSES_ROOT, HKEY_USERS** und **HKEY_CURRENT_CONFIG**.

Haben Sie mit dem Tool eine eigene ADM-Datei erzeugt, so können Sie diese ASCII-Datei mit jedem beliebigen Editor öffnen, während die originalen ADM-Dateien sich nur mit speziellen Editoren wie z. B. Notepad öffnen und bearbeiten lassen. Außerdem sind diese Dateien in einem Format, das leicht verständlich ist. Wenn Sie regelmäßig in PC-Magazinen, in Newslettern und in den Knowledge Base-Artikeln von Microsoft »herumschmökern«, werden Sie schnell weitere Tipps zum Betriebssystem Windows XP, zu Office XP/11 oder

zu anderen Anwendungen finden, die die Registry-Werte in den Zweigen **HKEY_LOCAL_MACHINE** oder **HKEY_CURRENT_USER** betreffen. Haben Sie eine eigene ADM-Datei mit dem Tool **Registry System Wizard e**rstellt und deren einfachen Aufbau verstanden, so wird es Ihnen leicht fallen, diese eigene ADM-Datei um die gewünschten **Registry-Keys** zu erweitern. Somit sind Sie in der Lage, all diese Veränderungen zentral über das Active Directory zu steuern. So werden Sie schnell zum Experten im Erstellen von eigenen Gruppenrichtliniendateien.

13.2 Die Struktur von Vorlagedateien für Gruppenrichtlinien

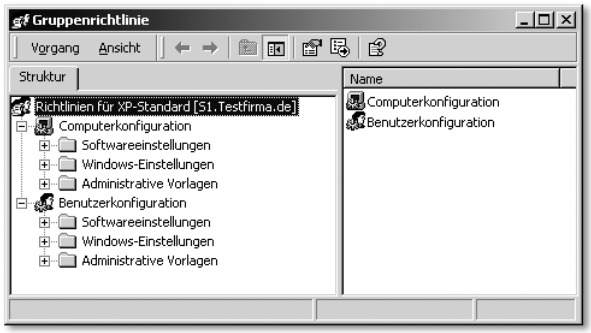
Eine ganz einfache Gruppenrichtliniendatei, die nur eine einzige Richtlinie enthält, mit der der Registry-Wert **HKEY_CURRENT_USER\Software\Microsoft\Windows NT\Current Version\Network\Persistent Connections** auf **YES** oder **NO** eingestellt werden kann, hat zum Beispiel folgendes Aussehen:

```
CLASS MACHINE
CATEGORY "APIPA-Funktion fuer DHCP-Betrieb deaktivieren"
   KEYNAME "System\CurrentControlSet\Services\TCPIP\Parameters"
   POLICY "IpAutoConfigurationEnabled"
   VALUENAME "IpAutoConfigurationEnabled"
   ValueON NUMERIC "0"
   ValueOff NUMERIC "1"
   Part "Wenn kein DHCP-Server beim Start eines Windows XP.Cli-
         ents verfügbar ist, "Text End Part
   Part "verliert der Client die zuletzt zugewiesene IP-Adresse
         und nimmt "Text End Part
   Part "eine IP-Adresse zwischen 169.254.0.0 und
         169.254.254.254 an. "Text End Part
   Part "Durch das Aktivieren dieser Richtlinie erreichen Sie,
         dass der Windows XP Client "Text End Part
   Part "zumindest so lange die vom DHCP-Server zugewiesene IP-
         Adresse beibehält, "Text End Part
   Part "bis diese laut Lease-Dauer noch gültig ist. "Text End
         Part
   END POLICY
END CATEGORY
CATEGORY "Anmeldeoptionen unter Windows ein/ausblenden"
   KEYNAME "SOFTWARE\Microsoft\Windows NT\CurrentVersion\
            Winlogon"
```

```
   POLICY "ShowLogonOptions"
   VALUENAME "ShowLogonOptions"
   ValueON NUMERIC "1"
   ValueOFF NUMERIC "0"
   Part "Wenn Sie diese Funktion aktivieren, werden die erwei-
         terten Optionen beim Start "Text End Part
   Part "sofort angezeigt und der Button Optionen muss nicht erst
         gedrückt werden. "Text End Part
   Part "Dies ist hilfreich, wenn man sich an unterschiedlichen
         Domänen anmelden muss. "Text End Part
   END POLICY
END CATEGORY
CLASS USER
CATEGORY "Netzwerkverbindungen nicht zwischen Sitzungen spei-
chern"
   KEYNAME "Software\Microsoft\Windows NT\CurrentVersion\Net-
            work\Persistent Connections"
   POLICY "SaveConnections"
   VALUENAME "SaveConnections"
   ValueON "YES"
   ValueOFF "NO"
   Part "Standardmäßig ist unter Windows diese Funktion akti-
         viert.  "Text End Part
   Part "Das bedeutet, dass die Erstellung von Netzwerkverbin-
         dungen  "Text End Part
   Part "gespeichert wird und bei einem Neustart des Rechners
        "Text End Part
   Part "automatisch versucht wird, diese Verbindung wieder
        "Text End Part
   Part "aufzubauen. Gerade bei Notebooks die nicht immer am
        "Text End Part
   Part "Netzwerk angeschlossen sind, kann das zu unnötigen
        "Text End Part
   Part "Fehlermeldungen führen, weshalb Sie hier lieber diese
        "Text End Part
   Part "Funktion deaktivieren sollten.  "Text End Part
   END POLICY
END CATEGORY
```

Das Schema einer ADM-Datei ist also Folgendes: Eine ADM-Datei besteht aus den beiden Kategorien **CLASS MACHINE** und/oder **CLASS USER**. Alle Richtli-

nien, die unter **CLASS MACHINE** stehen, tauchen später unter **Computerkonfiguration · Administrative Vorlagen** auf und führen zu Änderungen im Zweig **HKEY_LOCAL_MACHINE** der Registrierdatenbank.



Alle Richtlinien, die unter **CLASS USER** stehen, tauchen später unter **Benutzerkonfiguration · Administrative Vorlagen** auf und führen zu Änderungen im Zweig **HKEY_CURRENT_ USER** der Registrierdatenbank.

Die Kategorien **CLASS MACHINE** und **CLASS USER** können nun über den Ausdruck **CATEGORy Kategoriename ... END CATEGORY** wiederum in Unterkategorien unterteilt werden.

Als Nächstes folgt der **KEYNAME**, der den Schlüssel in der Registry angibt, in dem sich die nachfolgenden **VALUENAMES** befinden. Danach folgt mindestens eine Richtlinie mit je einem **VALUENAME**.

Jede Richtlinie wird durch das Schlüsselwort **POLICY** eingeleitet und durch **END POLICY** beendet. Die Richtlinien können einen beschreibenden Text erhalten. Dieser beginnt mit **Part** und endet mit **Text End Part**. Der beschreibende Text kann jedoch auch in einem separaten Abschnitt mit der Bezeichnung **[Strings]** ganz am Ende der ADM-Datei zusammengefasst werden. Diese Möglichkeit wird weiter unten beschrieben. Sie finden hierzu auch zwei ADM-Beispieldateien namens **WindowsExplorer.adm** und **ExchangeProvider.adm** auf dem beiliegenden Datenträger.

Das Schema sieht also wie folgt aus:

```
CLASS MACHINE
CATEGORY "erste Kategorie für HKEY_LOCAL_MCHINE"
   KEYNAME "Registrypfad"
   POLICY "Beschreibung der ersten Richtlinie"
   VALUENAME "Name des Wertes"
   ValueON NUMERIC "0"
```

```
   ValueOff NUMERIC "1"
   Part "beschreibender Text "Text End Part
   Part "aufgeteilt auf mehrere Zeilen "Text End Part
   END POLICY
   POLICY "Beschreibung der zweiten Richtlinie"
   VALUENAME "Name des Wertes"
   ValueON NUMERIC "0"
   ValueOff NUMERIC "1"
   Part "beschreibender Text "Text End Part
   Part "aufgeteilt auf mehrere Zeilen "Text End Part
   END POLICY
END CATEGORY
CATEGORY "zweite Kategorie für HKEY_LOCAL_MACHINE"
   KEYNAME "Registrypfad"
   POLICY "Beschreibung der Richtlinie"
   VALUENAME "Name des Wertes"
   ValueON NUMERIC "0"
   ValueOff NUMERIC "1"
   Part "beschreibender Text "Text End Part
   Part "aufgeteilt auf mehrere Zeilen "Text End Part
   END POLICY
END CATEGORY
CLASS USER
CATEGORY "erste Kategorie für HKEY_CURRENT_USER"
   KEYNAME "Registrypfad"
   POLICY "Beschreibung der Richtlinie"
   VALUENAME "Name des Wertes"
   ValueON NUMERIC "0"
   ValueOff NUMERIC "1"
   Part "beschreibender Text "Text End Part
   Part "aufgeteilt auf mehrere Zeilen "Text End Part
   END POLICY
   POLICY "Beschreibung der nächsten Richtlinie"
   VALUENAME "Name des Wertes"
   ValueON NUMERIC "0"
   ValueOff NUMERIC "1"
   Part "beschreibender Text "Text End Part
   Part "aufgeteilt auf mehrere Zeilen "Text End Part
   END POLICY
END CATEGORY
```

Mögliche Werttypen können sein:

REG_DWORD-Werte, das sind Binärwerte mit Zahlen wie **0**, **1**, **2**. Ein Beispiel:

```
CLASS MACHINE
CATEGORY "Warnmeldung wenn Festplatte voll"
   KEYNAME "System\CurrentControlSet\Services\LanmanServer\Para-
            meters"
   POLICY "Wert: DiskSpaceThreshold"
   PART "in Prozent" Numeric Required
   Min 0 Max 99
   ValueName "DiskSpaceThreshold"
   Default "10"
   END PART
   END POLICY
END CATEGORY
CATEGORY "APIPA-Funktion fuer DHCP-Betrieb deaktivieren"
   KEYNAME "System\CurrentControlSet\Services\TCPIP\Parameters"
POLICY "IpAutoConfigurationEnabled"
   VALUENAME "IpAutoConfigurationEnabled"
   ValueON NUMERIC "0"
   ValueOff NUMERIC "1"
   END POLICY
END CATEGORY
```


RG_SZ-Werte, das sind Zeichenfolgewerte wie **C:\Programme**. Ein Beispiel:

```
CLASS MACHINE
CATEGORY "Standardinstallationspfad für Anwendungen verändern"
   KEYNAME "Software\Microsoft\Windows\CurrentVersion"
   POLICY "ProgramFilesDir"
   ValueON ""
   ValueOff ""
   PART "Pfad:" EDITTEXT
   VALUENAME "ProgramFilesDir"
   DEFAULT "C:\Programme"
   END PART
   END POLICY
END CATEGORY
```

REG_EXPAND_SZ-Werte, das sind Werte, die mittels Variableninhalte zur Laufzeit aufgelöst werden. Ein Beispiel:

```
CLASS MACHINE
CATEGORY "Standardinstallationspfad verändern"
   KEYNAME "Software\Microsoft\Windows\CurrentVersion"
```

```
   POLICY "ProgramFilesPath"
   Part "Pfad:" EDITTEXT
   VALUENAME "ProgramFilesPath"
   DEFAULT "%ProgramFiles%"
   REQUIRED
   #if VERSION >= 2
   EXPANDABLETEXT
   #endif
   END PART
   END POLICY
END CATEGORY
```

REG_EXPAND_SZ-Werte wurden erst ab Windows 2000 unterstützt. Darum finden Sie in obigem Beispiel die Abfrage **#if VERSION >= 2 EXPANDABLETEXT #endif**. Die Angabe eines Defaultwertes, wie Sie ihn in den obigen Beispielen finden, ist nicht zwingend.

Sie können jedoch auch ein anderes Format verwenden, bei dem die beschreibenden Texte in einem separaten Abschnitt **[strings]** am Ende der Vorlagedatei zusammengefasst werden, statt direkt im zugehörigen Policy-Abschnitt zu erscheinen. Der Name der Richtlinie (**POLICY !!**) wird hierbei ebenso wie der beschreibende Text (**EXPLAIN !!**) durch zwei einleitende Rufzeichen referiert. Sowohl der eigentliche Richtlinienname als auch der beschreibende Text befinden sich dann im Abschnitt **[Strings]**. Im beschreibenden Text können Zeilenumbrüche durch **\n** (ein Zeilenumbruch) bzw. **\n\n** (zwei Zeilenumbrüche) angegeben werden. Ein Ausschnitt aus der beiliegenden Datei **WindowsExplorer.adm** verdeutlicht dieses Format:

```
CLASS USER
CATEGORY "Microsoft Explorer"
   CATEGORY "Ansicht"
      POLICY !!AnsichtoptionenfueralleOrdnerspeicher
          KEYNAME "Software\Microsoft\Windows\CurrentVer-
                   sion\Explorer\Advanced"
          EXPLAIN !!AnsichtoptionenfueralleOrdnerspeicher_Exp-
                    lain
          VALUENAME "ClassicViewState"
          VALUEON NUMERIC 1
          VALUEOFF NUMERIC 0
      END POLICY
      POLICY !!Dateierweiterunganzeigen
```

```
         KEYNAME "Software\Microsoft\Windows\CurrentVer-
                  sion\Explorer\Advanced"
         EXPLAIN !!Dateierweiterunganzeigen_Explain
         VALUENAME "HideFileExt"
         VALUEON NUMERIC 0
         VALUEOFF NUMERIC 1
      END POLICY
      POLICY !!geschuetzteSystemdateienausblenden
         KEYNAME "Software\Microsoft\Windows\CurrentVer-
         sion\Explorer\Advanced"
         EXPLAIN !!geschuetzteSystemdateienausblenden_Explain
         VALUENAME "ShowSuperHidden"
         VALUEON NUMERIC 0
         VALUEOFF NUMERIC 1
      END POLICY
   END CATEGORY ; "Ansicht"
END CATEGORY ; "Microsoft Explorer"
[strings]
AnsichtoptionenfueralleOrdnerspeicher="eingestellte Ansichtopti-
onen für alle Ordner übernehmen"
AnsichtoptionenfueralleOrdnerspeicher_Explain="Wenn diese Ein-
stellung aktiviert ist, werden Einstellungen, die in einem Ord-
ner vorgenommen werden, für jeden Ordner übernommen. Die
Aktivierung ist sinnvoll.\n\nBei deaktivierter Einstellung wer-
den die Einstellungen nicht für jeden Ordner gespeichert, son-
dern nur für den aktuellen Ordner."
Dateierweiterunganzeigen="Dateierweiterung auch bei bekannten
Dateitypen anzeigen"
Dateierweiterunganzeigen_Explain="Wenn diese Einstellung akti-
viert ist, werden alle Dateiendungen der Dateien angezeigt. Auch
Endungen wie doc, xls, exe und com werden wieder angezeigt. Es
ist sinnvoll, diese Richtlinie zu aktivieren.\n\nBei deaktivier-
ter Einstellung werden Dateiendungen bei bekannten Dateitypen
ausgeblendet."
```

Beachten Sie, dass das Ende einer Kategorie durch den Ausdruck **END CATEGORY** angezeigt wird. Wenn eine ADM-Datei viele Kategorien enthält und diese auch noch ineinander verschachtelt sind, sollte der Ausdruck **END CATEGORY** durch einen mit einem Semikolon eingeleiteten Kommentartext ergänzt werden (z.B. **END CATEGORY ; Name der Kategorie**). Besteht der Name einer Kategorie aus mehreren Worten, so muss er in Anführungszeichen stehen.

Die von Microsoft gelieferten ADM-Dateien haben unterschiedliche Formate. Die Microsoft Office 2000- bzw. Office XP-ADM-Dateien, die nicht zum Lieferumfang der Office-Version gehören, sondern nach Installation des zugehörigen Office Resource Kits im Verzeichnis **C:\Windows\Inf** landen, können wieder mit beliebigen Editoren geöffnet werden. Ihr Format ist dasselbe, welches Sie sehen, wenn Sie mit dem Registry System Wizard eine eigene ADM-Datei erstellen. Leider enthalten die Microsoft Office-ADM-Dateien zumindest in der mir vorliegenden Version keine erklärenden Texte für die einzelnen Richtlinien, sodass man oft nur raten kann, was sie bewirken.

Die zum Lieferumfang von Windows 2000 bzw. Windows XP gehörenden ADM-Dateien können Sie mit **Notepad.exe** ansehen oder sogar verändern, nicht aber mit vielen anderen Editoren wie z. B. dem DOS-Editor **edit.com**, den Sie im Verzeichnis **SYSTEM32** finden, oder dem Editor des Norton Commander für Windows 2000. Die die einzelnen Richtlinien beschreibenden Texte stehen ganz am Ende der ADM-Datei in einem speziellen Abschnitt mit der Bezeichnung **[Strings]**.

Zwei wichtige Tipps

Nehmen Sie keine Veränderungen an den original ADM-Dateien von Microsoft vor. Kommt irgendwann ein neues Service Pack heraus, so hat dieses eventuell auch neue ADM-Dateien. Wenn Sie das Service Pack einspielen, gehen eventuell die von Ihnen vorgenommenen Änderungen wieder verloren, bzw. Sie müssen die Änderungen mühselig in die neuen ADM-Dateien des Service Packs integrieren, um die Verbesserungen der neuen ADM-Dateien nutzen zu können und Ihre Anpassungen nicht gleichzeitig zu verlieren.

Erstellen Sie sich stattdessen eigene ADM-Dateien mit sprechenden Namen. Testen Sie die eigenen ADM-Dateien in einer Testdomäne sorgfältig aus. Kopieren Sie diese Dateien auf einen der Domänencontroller in das Verzeichnis **C:\Winnt\inf** und laden Sie die selbst erstellen ADM-Dateien hinzu.

Wenn Sie wissen möchten, welchen Registry Key eine Richtlinie der von Microsoft zum Betriebssystem mitgelieferten Vorlagedateien verändert, so schreiben Sie den Namen der Richtlinie bzw. den beschreibenden Text auf, öffnen die entsprechende ADM-Datei mit **Notepad.exe** und suchen nach dem Namen bzw. nach dem beschreibenden Text der Richtlinie. Sie werden dann irgendwo im Abschnitt **[Strings]** fündig. Gehen Sie an der Fundstelle zum Anfang der

Zeile und notieren Sie den Wert vor dem Gleichheitszeichen. Suchen Sie die ADM-Datei vom Anfang beginnend nach diesem notierten Wert durch. Sie finden eine Zeile, die mit **POLICY !!notierter Wert** beginnt, und direkt darunter den **KEYNAME** und **VALUENAME**. Jetzt müssen Sie nur noch überprüfen, ob dieser **KEYNAME** unterhalb von **CLASS MACHINE** oder **CLASS USER** steht, um zu wissen, ob der Wert in der Registrierdatenbank im Zweig **HKEY_LOCAL_MACHINE** oder **HKEY_CURRENT_USER** zu finden ist.

13.3 Die selbst erstellte Gruppenrichtliniendatei »WindowsXP-HLM« nutzen

Auf der Buch-CD finden Sie zwei ADM-Dateien mit den Bezeichnungen **WindowsXP-HLM.ADM** und **WindowsXP-HCU.ADM**, mit denen weitere interessante Einstellungen in der **Registry** von Windows XP vorgenommen werden können. Die Richtlinie **WindowsXP-HLM.ADM** könnten Sie auf die Sub-OU **Computer** unterhalb der OU **Testfirma** anwenden, die Richtlinie **WindowsXP-HCU**, die nur Änderungen am Zweig **HKEY_CURRENT_USER** vornimmt, könnte auf die Sub-OU **Benutzer** angewandt werden.

Die Gruppenrichtliniendatei **WindowsXP-HLM.ADM** nimmt nur Änderungen im Zweig **HKEY_LOCAL_MACHINE** der **Registry** vor. Deshalb wurden im Dateinamen die drei Buchstaben »HLM« verwendet. Die Gruppenrichtliniendatei **WindowsXP-HCU.ADM** nimmt nur Änderungen im Zweig **HKEY_CURRENT_USER** der **Registry** vor. Deshalb wurden im Dateinamen die drei Buchstaben »HCU« verwendet.

Kopieren Sie die beide Dateien in das Verzeichnis **C:\winnt\inf** bzw. **C:\Windows\inf** des Domänencontrollers. Öffnen Sie dann in der Sub-OU **Computer** der Organisationseinheit **Testfirma** die Gruppenrichtlinie **XP-Standardcomputer**, klicken Sie mit der rechten Maustaste in der Kategorie **Computerkonfiguration** auf **Administrative Vorlagen** und wählen Sie **Vorlagen hinzufügen/entfernen** und im Fenster **Vorlagen hinzufügen/entfernen** erneut auf **Hinzufügen**. Fügen Sie die Vorlage **WindowsXP-HLM** hinzu.

Sie sollten nun eine neue Kategorie mit der Bezeichnung **selbst erstellte Windows XP-Richtlinien für Hive HKEY_LOCAL_MACHINE** sehen. Wenn Sie die Maus auf **Administrative Vorlagen** stellen und dann unter **Ansicht** die Option **Nur Richtlinien anzeigen** nicht deaktiviert ist, so sehen Sie die einzelnen Richtlinien nicht und können sie auch nicht einstellen!

Wichtiger Hinweis: Wenn die Maus ganz oben auf **Richtlinie für XP-Standard …** steht, sehen Sie unter Ansicht nicht die Option **Nur Richtlinien anzeigen**, sondern **DC-Optionen**!

Echte und unechte Gruppenrichtlinien

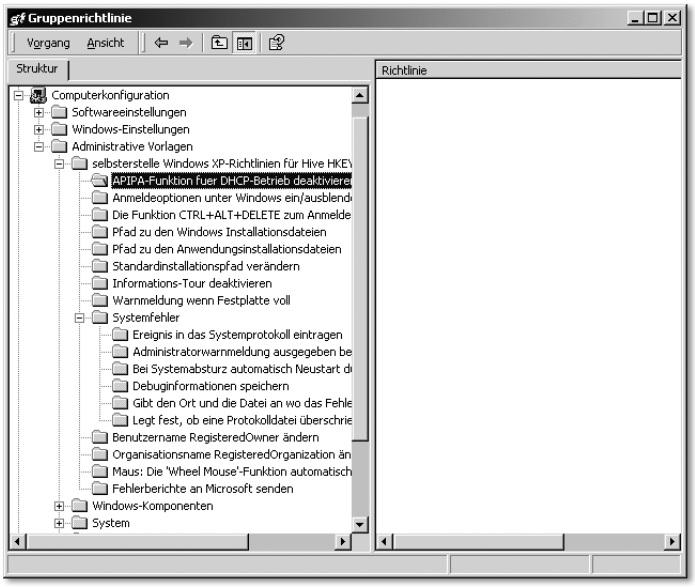
Es gibt zwei Arten von Richtlinien, nennen wir sie »echte« und »unechte« Richtlinien: Bei den echten Richtlinien werden Änderungen in einem der folgenden Registry-Keys vorgenommen:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies,
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\policies,

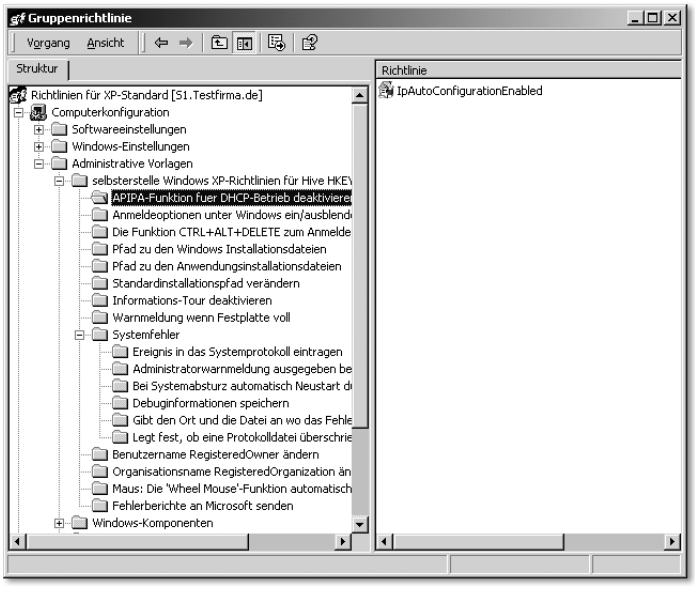
HKEY_CURRENT_USER\SOFTWARE\Policies,
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current Version\policies.

Der Anwender hat auf Unterschlüssel und Werte dieser echten Richtlinien kein Recht zur Änderung und kann deshalb diese Einstellungen nicht manipulieren. Wenn Sie jedoch z.B. selbst eine ADM-Datei erstellen, können Sie auch beliebige andere Schlüssel und Werte in den Zweigen **HKEY_LOCAL_MACHINE** und **HKEY_CURRENT_USER** mit diesen ADM-Dateien steuern, Werte also, die nicht unterhalb der oben genannten Schlüssel liegen. Werte, die irgendwo im Schlüssel **HKEY_CURRENT_USER** liegen, kann der Anwender jedoch bis auf die oben genannten Schlüssel ändern. Folglich könnte ein Anwender zumindest während einer Sitzung diese Werte wieder ändern. Spätestens bei der nächsten Anmeldung greift jedoch die gesetzte unechte Richtlinie der von Ihnen erstellten **ADM-Datei** wieder.

Wenn Sie über das Snap-In **Active Directory-Benutzer und -Computer** eine Gruppenrichtlinie bearbeiten wollen und eine ADM-Datei mit unechten Richtlinien geladen haben, so sehen Sie die unechten Richtlinien per Defaulteinstellung nicht.



Die Ursache: Unter Ansicht ist standardmäßig die Option **Nur Richtlinien anzeigen** aktiviert. Stellen Sie die Maus auf **Administrative Vorlagen**, bevor Sie den Menüpunkt **Ansicht** anwählen. Wenn die Maus ganz oben auf **Richtlinien für …** steht, sehen Sie unter **Ansicht** nicht die Option **Nur Richtlinien anzeigen**, sondern **DC-Optionen**! Erst wenn Sie die Option **Nur Richtlinien anzeigen** deaktivieren, sehen Sie auch die unechten Richtlinien.



Die dem Datenträger beiliegende Gruppenrichtliniendatei **WindowsXP-HLM.ADM** ermöglicht die Einstellung folgender Richtlinien:

APIPA-Funktion fuer DHCP-Betrieb deaktivieren

Wenn Sie den Clients die IP-Adressen über einen DHCP-Server dynamisch zuweisen, der DHCP-Server ausfällt und kein Ersatz-DHCP-Server verfügbar ist, so sollte der Client die zugewiesene DHCP-Adresse eigentlich über die Gültigkeitsdauer der Lease behalten. Wurde in den Optionen des DHCP-Servers z. B. eine Gültigkeitsdauer von 30 Tagen eingetragen, und hat der Client zuletzt vor 10 Tagen eine neue IP-Adresse zugewiesen bekommen, so ist diese IP-Adresse noch für 20 Tage gültig.

Ein Windows 2000 Professional-Computer wird beim Starten auch keine Probleme machen, wenn der einzige DHCP-Server aus irgendwelchen Gründen momentan nicht verfügbar ist. Windows XP-Clients vergessen per Default eine zugewiesene DHCP-Adresse, wenn der Registry-Key **IpAutoConfigurationEnabled** unter **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\TCPIP\Parameters** nicht auf **0** umgestellt wird.

Dieses Verhalten liegt an der neuen Funktion **Automatic Private IP Adressing (APIPA)**, mit der automatisch eine IP-Adresse aus dem Bereich 169.254.0.1 bis 169.254.255.254 und eine Subnetzmaske von 255.255.0.0 konfiguriert werden, wenn das TCP/IP-Protokoll für die dynamische Adressierung konfiguriert wird und kein DHCP-Server verfügbar ist.

Sie können dieses Verhalten leicht testen, indem Sie am Windows XP-Client das Netzwerkkabel abziehen und sich mit dem zwischengespeicherten Profil anschließend anmelden. Öffnen Sie eine DOS-Box und geben Sie den Befehl **ipconfig /all** ein. Sie erhalten eine Fehlermeldung und jedenfalls nicht die zuletzt als IP-Adresse vom DHCP-Server zugewiesene Adresse. Sobald Sie jedoch den Wert von **IpAutoConfigurationEnabled** von **1** auf **0** umgestellt haben und das Netzwerkkabel wieder eingesteckt haben, können Sie den Befehl **ipconfig /renew** und danach **ipconfig /all** eingeben bzw. den Computer neu starten und sich anmelden. Der Client erhält eine neue IP-Adresse vom DHCP-Server. Wenn Sie sich jetzt abmelden, erneut das Netzwerkkabel abziehen, sich dann wieder anmelden und erneut den Befehl **ipconfig /all** eingeben, stellen Sie fest, dass der Computer immer noch die vom DHCP-Server zugewiesene IP-Adresse besitzt.

Anmeldeoptionen unter Windows ein/ausblenden

Wenn Sie diese Funktion aktivieren, werden die erweiterten Optionen beim Start sofort angezeigt und die Schaltfläche Optionen muss nicht erst gedrückt werden. Dies ist besonders dann hilfreich, wenn man sich regelmäßig an unterschiedlichen Domänen anmelden muss.

Die Funktion Strg+Alt+Delete zum Anmelden deaktivieren

Wenn Sie diese Funktion aktivieren, müssen die Anwender zum Anmelden nicht mehr die Tastenkombination **Strg+Alt+Delete** drücken. Dies ist jedoch eine kleine Sicherheitslücke, da durch diese Tastenkombination sichergestellt wird, dass ein eventuell noch in das System eingeklinkter Hacker die Verbindung verliert.

Pfad zu den Installationsdateien und Pfad zu den Anwendungsinstallationsdateien

Wenn unter Windows XP oder Windows 2000 Komponenten nachinstalliert werden müssen, so sucht das Betriebssystem in den Pfaden, die unter folgenden Schlüsselwerten angegeben sind:

Software\Microsoft\Windows NT\CurrentVersion: Sourcepath,
Software\Microsoft\Windows\CurrentVersion\Setup: Sourcepath,
Software\Microsoft\Windows\CurrentVersion\Setup: Installation Sources,
Software\Microsoft\Windows\CurrentVersion\Setup: ServicePackSourcePath.

Je nachdem, ob Sie das Betriebssystem von einer CD oder von einem RIS-Server installiert haben, stehen in diesen Schlüsseln Inhalte wie **E:**, **E:\I386** oder

\\S1\RemInst\Setup\German\IMAGES\WindowsXP. Diese Pfadeinträge sollten Sie jedoch bei Bedarf anpassen. In Kapitel 10 »Das Loginskript« finden Sie den Abschnitt »Software aus einem zentralen Software-Archive installieren«, in dem begründet wird, warum auf mindestens einem Server jedes Standorts ein Software-Archiv angelegt bzw. zwischen verschiedenen Servern synchronisiert und jeweils z.B. unter dem Namen **Install** freigegeben werden sollte. Wenn außerdem über das Loginskript sichergestellt ist, dass immer dasselbe Netzlaufwerk mit jeweils dem Software-Archiv des Servers am jeweiligen Standort verbunden ist (z.B. durch den Befehl **net use u: \\ServerA1\install** am Standort A und durch den Befehl **net use u: \\ServerB1\install** am Standort B), so können Sie über die beiden Richtlinien **Pfad zu den Installationsdateien** und **Pfad zu den Anwendungsinstallationsdateien** die Registry-Werte auf **u:\WindowsXP** umlegen. Vorausgesetzt, auf diesen Software-Archiv-Servern befindet sich jeweils eine administrative Installation von Windows XP mit integriertem Service Pack im Verzeichnis **WindowsXP** unterhalb der Freigabe **Install**, so werden nachzuinstallierende Treiberdateien immer gefunden, und Sie müssen nicht mehr mit den Installations-CDs zu den Computern laufen. Das ist besonders dann wichtig, wenn die Computer keine eingebauten CD-Laufwerke haben.

Wenn Sie das Betriebssystem Windows 2000 oder Windows XP von einem RIS-Server installiert haben, wird in diesen Registry-Werten ein Pfad wie z.B. **\\S1\RemInst\Setup\German\ IMAGES\WindowsXP** stehen. Nach der Installation der Standardanwendungen werden Sie später ein Komplettabbild ziehen und auf dem RIS-Server ablegen. Wenn dieser Server **S1** heißt und am Standort A steht, jedoch ein mit diesem Komplettabbild bespielter Computer später am Standort B steht, so führt dies zu folgendem Problem: Selbst wenn Sie am Standort B ebenfalls einen RIS-Server aufstellen, würde der Computer bei dem Versuch, eine Betriebssystemkomponente oder eine Komponente von Office XP/11 nachzuinstallieren, nach der Originalquelle suchen und dann wahrscheinlich eine Verbindung über die langsame WAN-Verbindung aufmachen und von dem Server die benötigten Treiber herunterladen, von dem ursprünglich Windows XP bzw. Office XP/11 installiert wurde. Wenn Sie jedoch bei allen Installationen immer ein Unterverzeichnis der fest definierten Laufwerkszuweisung **U:** verwenden, und folglich alle Treiber bei einer Nachinstallation unter **U:\WindowsXP**, **U:\OfficeXP** (bzw. **U:\Office11**) usw. gesucht werden, so ist sichergestellt, dass immer der Software-Archiv-Server vor Ort und nicht der ursprünglich bei der Erstinstallation als Quelle verwendete Server kontaktiert wird.

Standardinstallationspfad verändern

Drei weitere Richtlinien finden Sie in der Datei **WindowsXP-HLM.adm**, die Sie wahrscheinlich nicht benötigen werden. Dennoch ist es interessant zu wissen, wo in der Registry die Verknüpfung liegt, dass für die Installation weiterer Anwendungen immer das Verzeichnis **C:\Programme** und für gemeinsam verwendete Komponenten das Verzeichnis **C:\Programme\Gemeinsame Dateien** vorgeschlagen wird.

Unter **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version** finden Sie die Schlüssel **ProgramFilesDir** mit dem Defaultwert **C:\Programme**, **ProgramFilesPath** mit dem Defaultwert **%ProgramFiles%** und **CommonFilesDir** mit dem Defaultwert **C:\Programme\Gemeinsame Dateien**. Hier finden Sie außerdem den Schlüssel **MediaPath** mit dem Defaultwert **C:\WINDOWS\Media**. Wenn Sie irgendwann aus irgendeinem Grund diese Pfade umlegen wollen, wissen Sie nun, wo Sie suchen müssen.

Informations-Tour deaktivieren

Wenn Sie diese Richtlinie aktivieren, wird für einen neu eingerichteten Anwender bei der ersten Anmeldung unter Windows XP nicht mehr gefragt, ob die Windows XP-Tour gestartet werden soll. Dazu ändert die Richtlinie unter **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Applets\Tour** den Wert des Schlüssels **RunCount** von **1** auf **0** ab.

Warnmeldung wenn Festplatte voll

Wenn auf der Systempartition von Windows XP weniger als 10 % frei sind, erhält der Anwender regelmäßig eine Warnmeldung, und es können keine weiteren Anwendungen mehr installiert werden, bevor nicht aufgeräumt wird oder andere Anwendungen deinstalliert werden. Bei einer 10 GByte-Partition bedeutet das aber, dass trotz 1 GByte freien Speichers zu wenig Speicherplatz gemeldet wird. Die Aktivierung der Richtlinie **Warnmeldung wenn Festplatte voll** fordert Sie auf, einen Wert zwischen **0** und **99** einzugeben, wodurch Sie den **Defaultwert** von **10** (gemeint ist damit 10 % der Partition) vermindern können. Dadurch wird unter **KEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters** der Schlüssel **DiskSpaceThreshold** neu gesetzt. Ein Wert von **5** scheint angemessen. Selbst bei einer 2 GByte kleinen Partition sind 5 % davon noch 100 MByte freier Speicherplatz. Vor dem Unterschreiten dieses Grenzwertes wäre eine Warnmeldung übertrieben.

Systemfehler

Über die Richtlinien der Kategorie können Sie von zentraler Stelle aus für alle Computer der Organisationseinheit **Computer** die Windows XP-Einstellungen steuern, die das Verhalten bei einem Systemabsturz bestimmen. Wenn Sie in Windows XP über **Start · Einstellungen · Systemsteuerung · System** die Systemsteuerung starten, die Registerkarte **Erweitert** auswählen und im unteren Bereich **Starten und Wiederherstellen** die Schaltfläche **Einstellungen** anwählen, finden Sie dort dieselben Einstellungsmöglichkeiten. Die Kategorie **Systemfehler** hat folgende Richtlinien:

- Ereignis in das Systemprotokoll eintragen
- Administratorwarnmeldung ausgegeben bei Systemabsturz
- Bei Systemabsturz automatisch Neustart durchführen
- Debuginformationen speichern
- Gibt den Ort und die Datei an wo das Fehlerlog abgelegt werden soll
- Legt fest, ob eine Protokolldatei überschrieben werden darf

Ich schlage Ihnen vor, alle Richtlinien zu aktivieren und nur die Richtlinie **Debuginformationen speichern** zu deaktivieren. Ist nämlich die Richtlinie **Debuginformationen speichern** aktiviert, so wird unter **C:\Windows** bei einem Systemabsturz ein mindestens 64 KByte großes Speicherabbild erstellt. Dieser Vorgang benötigt Zeit und Speicherplatz. Wenn Sie jedoch nicht in der Lage sind, dieses Speicherabbild zu interpretieren (und das können oft nur Experten vom technischen Kundendienst), nützt Ihnen das Abbild nichts. Wenn ein Windows XP-Computer regelmäßig abstürzt, werden Sie ihn so oder so austauschen und ihn in Ruhe auf Herz und Nieren prüfen: Führen Sie eine Neuinstallation durch oder tauschen Sie Hardwarekomponenten aus, wenn der Fehler immer noch auftritt.

Benutzername RegisteredOwner und Organisationsname RegisteredOrganization ändern

Angenommen, Sie haben das RIPrep-Abbild von Windows XP mit allen Standardanwendungen auf vielen Computern in der Hauptniederlassung und einigen Filialen installiert, und plötzlich fusioniert Ihre Company und bekommt einen neuen Firmennamen.

Nehmen wir ferner an, Sie wollen ein und dasselbe Komplettabbild für verschiedene Tochterfirmen verwenden, die jedoch unterschiedliche Firmennamen haben.

Und stellen Sie sich vor, Sie haben bei der Installation von Windows XP auf dem Mustercomputer einen bestimmten Namen eingegeben wie z. B. »Systemverwalter«, möchten jedoch nach der Verteilung des Komplettabbildes auf allen Computern diesen Namen ändern.

Mit den beiden Richtlinien **Benutzername RegisteredOwner ändern** und **Organisationsname RegisteredOrganization ändern** geht das sehr komfortabel von Ihrem Arbeitsplatz aus. Diese Richtlinien ändern unter **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion** die Schlüssel **RegisteredOrganization** und **RegisteredOwner**.

Die »Wheel Mouse«-Funktion automatisch erkennen

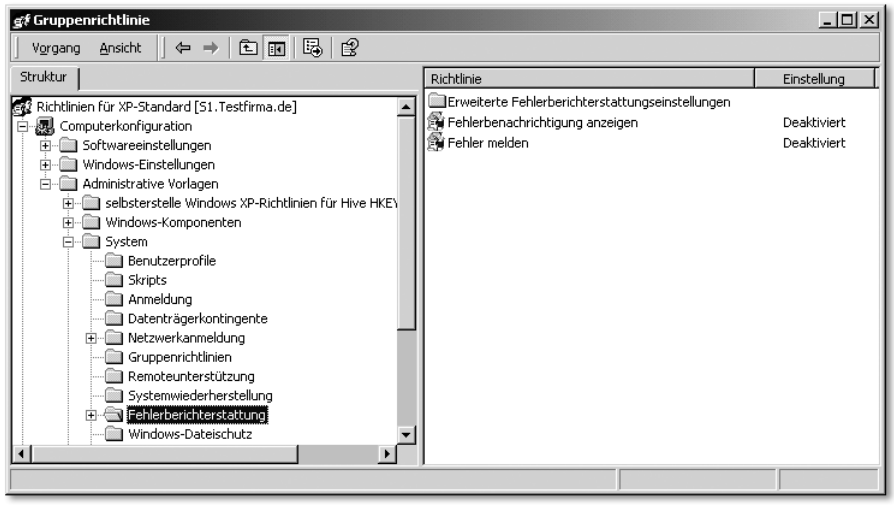
Wenn ein Computer, an dem eine Maus ohne Rad installiert ist, mit Windows XP installiert wird und nachträglich eine Maus mit Rad (Wheel Mouse) angeschlossen wird, so funktioniert das Rad nicht. Erst wenn der Schlüssel unter **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\i8042-prt\Parameters** der DWord-Schlüssel **EnableWheelDetection** erstellt und auf **1** gesetzt wird, wird das Rad erkannt und ist funktionstüchtig.

Wichtiger Tipp: Sie sollten dennoch den Computer, auf dem Sie die Musterkonfiguration aufsetzten und von dem Sie später ein Abbild ziehen, vor der Installation mit einer Wheel Mouse ausrüsten, um allen Problemen aus dem Weg zu gehen. Wird später ein Computer, an dem keine Wheel Mouse angeschlossen ist, mit diesem Abbild bespielt, so ist das unproblematisch. Umgekehrt können Sie durch diesen Registry-Key zwar eine Wheel Mouse rudimentär aktivieren, jedoch die Optionen des Rades nicht unbedingt einstellen.

Fehlerbericht an Microsoft senden

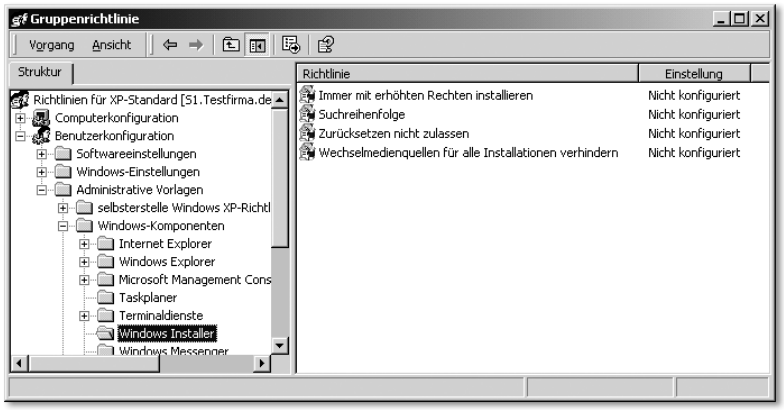
Deaktivieren Sie die beiden Richtlinien **DoReport** und **ShowUI**, damit keine Fehlermeldungen automatisch an Microsoft gesendet werden. Damit wird unter **Systemsteuerung · System** in der Registerkarte **Erweitert** das Fenster **Fehlerberichterstattung** vorkonfiguriert, das Sie sehen, wenn Sie auf die Schaltfläche **Fehlerberichterstattung** klicken.

Diese Richtlinien wurden zwar schon unter **Administrative Vorlagen · System · Fehlerberichterstattung** deaktviert, doch zumindest in meiner Testumgebung wurde bei der Überprüfung mittels des Fensters **Fehlerberichterstattung** unter **Systemsteuerung · System · Erweitert · Fehlerberichterstattung** das gewünschte Ziel erst erreicht, als diese Richtlinie zusätzlich in die selbst erstellte Vorlagedatei **WindowXP-HLM.ADM** aufgenommen wurde.



13.4 Die selbst erstellte Gruppenrichtliniendatei »WindowsXP-HCU« nutzen

Im letzten Unterkapitel wurde erläutert, wie die Gruppenrichtlinie basierend auf der Vorlage **WindowsXP-HLM.ADM** auf die Organisationseinheit **Computer** unterhalb der Organisationseinheit **Testfirma** angewendet wird. Jetzt



Solange Sie jedoch keine MSI-Pakete über die Kategorie **Benutzerkonfiguration · Softwareeinstellungen** hinzufügen, müssen Sie mit diesen Richtlinien auch nicht herumtesten. Wahrscheinlich wäre es nicht schädlich, Richtlinien wie **Immer mit erhöhten Rechten installieren** zu aktivieren, um Rechteprobleme zu beseitigen, die bei der Installation eventuell auftauchen. Meine Zuweisung des Office XP-Standardpakets (die Datei **proplus.msi** mit der Transformationsdatei **standard.mst**) lief jedoch auch ohne die Konfiguration einer der Richtlinien in der Kategorie **Windows Installer** fehlerlos durch.

14.3 Die Office-Gruppenrichtlinien nutzen

Wenn Sie diese Dokumentation lesen, ist wahrscheinlich schon Office 2003 auf dem Markt verfügbar. Zwar lag auch dem Autor bereits eine Beta-Version vor, doch gehörten die Gruppenvorlagedateien nicht zum Lieferumfang. Es ist zu vermuten, dass wie unter Office 2000 und Office XP die Gruppenrichtlinien-Vorlagedateien zum Lieferumfang des Office 2003 Resource Kits gehören werden. Dennoch sollten Sie dieses Kapitel nicht auslassen, denn die generelle Vorgehensweise zur Analyse von Office-Gruppenrichtlinien wird auch für die nächste Office-Version anwendbar sein. Die Vorlagedateien werden wahrscheinlich **xxx11.adm** heißen und einige weitere Richtlinien enthalten. Es wird ein neues Office 11 Resource Kit geben. Die Einträge, die von Office 2003 in die Registrierdatenbank vorgenommen werden, werden unter **HKEY_CURRENT_USER\Software\Microsoft\Office\11.0** zu finden sein, doch an der generellen Technik hat sich zwischen Office 2000 und Office XP nichts verändert, und so wird es wahrscheinlich auch zwischen Office XP und Office 11 sein. Generell geht es in diesem Buch weniger um die Installation einer bestimmten Version von Windows Server, Exchange Server oder Office, sondern darum, zu erlernen, wie man methodisch an die Installation dieser Produkte herangehen kann.

Nach der Installation des Office Resource Kits auf dem Server finden Sie im Verzeichnis **C:\Winnt\inf** bzw. **C:\Windows\inf** weitere ADM-Dateien, die zu Office XP gehören und zu einer Gruppenrichtlinie hinzugefügt werden können. Es handelt sich um folgende Dateien:

Access10.adm	Richtlinien für Access 2002
Excel10.adm	Richtlinien für Excel 2002
Fp10.adm	Richtlinien für FrontPage 2002
Gal10.adm	Richtlinien für Office XP Clip Organizer
Instlr11.adm	Richtlinien für Windows Installer
Office10.adm	Richtlinien für den Office Resource Kit Custom Maintenance Wizard
Outlk10.adm	Richtlinien für Outlook 2002
Ppt10.adm	Richtlinien für PowerPoint 2002
Pub10.adm	Richtlinien für Publisher 2002
Wod10.adm	Richtlinien für Word 2002

Unter dem Nachfolgeprodukt Office 2003 werden diese Dateien statt der Versionsnummer »10« die Folgeversionsnummer »11« haben. Bis auf die Datei **INSTLR11.ADM**, die in meiner Installation des Office XP Resource Kits merkwürdiger Weise das alte Erstellungsdatum 06.06.2000 hat, haben alle anderen Dateien als Erstellungsdatum den 28.08.2001.

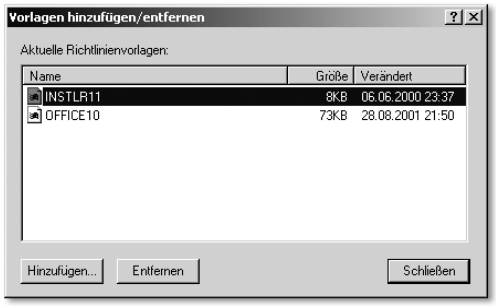
Es stellen sich folgende Fragen:

- Welche Funktionen haben diese Office XP-Vorlagedateien für Gruppenrichtlinien?
- Welche der Vorlagedateien sollten genutzt werden, ohne dass man in einem Wald von Gruppenrichtlinien den Überblick verliert?
- Welche der Vorlagedateien nehmen vorwiegend oder ausschließlich Änderungen an den Computereinstellungen vor, welche sind vorwiegend oder ausschließlich benutzerbezogen?
- Welche der Vorlagedateien sollen demnach auf eine Organisationseinheit, die nur Computer enthält, angewendet werden?
- Welche der Vorlagedateien sollen demnach auf eine Organisationseinheit, die nur Benutzer enthält, angewendet werden?

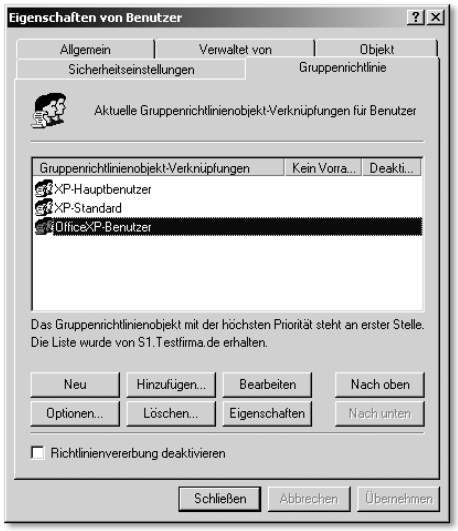
Öffnen Sie alle ADM-Dateien mit einem Editor und suchen Sie nach den Begriffen **class user** und dann nach **class machine**. Sie werden feststellen: Nur die Dateien instlr11.adm und office10.adm haben je eine Kategorie **class user**

und eine Kategorie **class machine**, die anderen Dateien haben keine Kategorie **class machine**. Das bedeutet, dass nur diese Vorlagedateien neue Richtlinien unter **Computerkonfiguration · Administrative Vorlagen** hinzufügen. Die restlichen Vorlagedateien stellen nur unter **Benutzerkonfiguration · Administrative Vorlagen** weitere Richtlinien bereit.

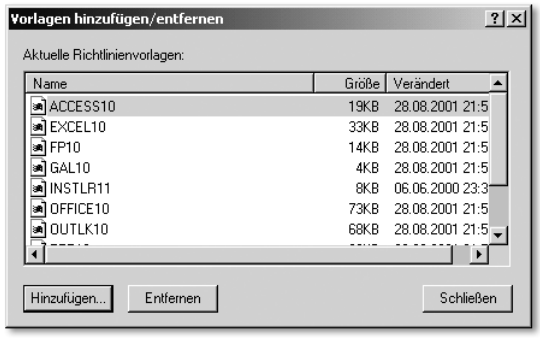
Um sich mit den neuen Gruppenrichtliniendateien vertraut zu machen, erstellen Sie in der Sub-OU **Computer** eine neue Gruppenrichtlinie mit dem Namen **OfficeXP-Computer**. Öffnen Sie die neue Gruppenrichtlinie, klicken Sie unter **Computerkonfiguration** die Kategorie **Administrative Vorlagen** mit der rechten Maustaste an und entladen Sie die Defaultvorlagen **conf**, **inetres** und **system**, damit Sie anschließend nur die Office-Richtlinien sehen. Fügen Sie anschließend die Vorlagen **instlr11.adm** und **office10.adm** hinzu.



Erstellen Sie in der Sub-OU **Benutzer** ebenso eine neue Gruppenrichtlinie, jedoch mit dem Namen **OfficeXP-Benutzer**.



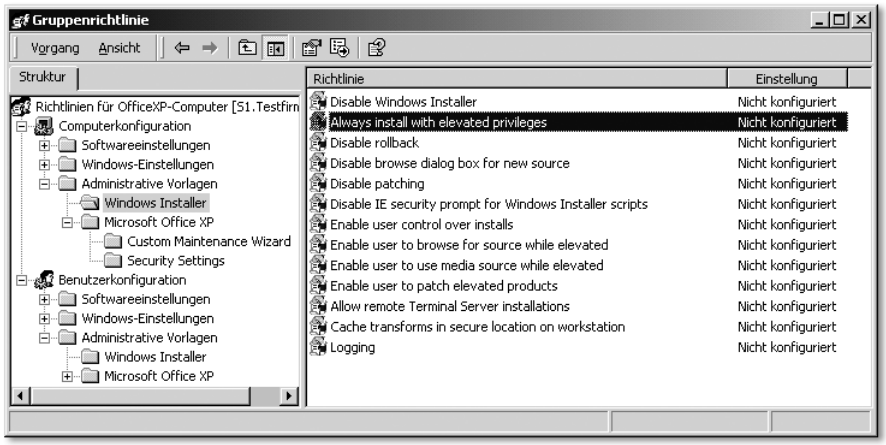
Öffnen Sie die neue Gruppenrichtlinie **OfficeXP-Benutzer**, wählen Sie unter **Benutzerkonfiguration** die Kategorie **Administrative Vorlagen** mit der rechten Maustaste an und entladen Sie die Defaultvorlagen **conf**, **inetres** und **system**. Fügen Sie anschließend die Vorlagen allen neu hinzugekommenen Office XP-ADM-Dateien hinzu.



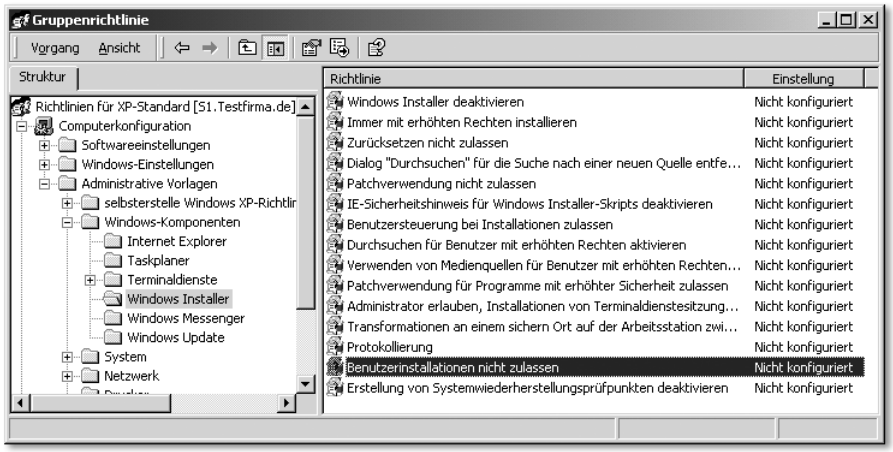
Sehen Sie sich nun die neuen Office XP-Richtlinien in beiden neuen Gruppenrichtlinien an, zuerst unter **Computerkonfiguration · Administrative Vorlagen**, danach unter **Benutzerkonfiguration · Administrative Vorlagen**. Besonders in der Kategorie **Benutzerkonfiguration** erhalten Sie eine Fülle neuer Richtlinien mit englischen Bezeichnungen und einer Registerkarte **Erklärung**, die leider keine einzige Beschreibung enthält! Alle Office XP-Gruppenrichtliniendateien sind nicht dokumentiert. Ihnen bleibt nur eines: Sehen Sie sich auf einem Computer, auf dem Office XP installiert ist, die Optionen der verschiedenen Anwendungen an. Mit ein wenig Fantasie werden Sie dann die Bedeutung vieler Office XP-Richtlinien erahnen können.

14.4 Office XP-Richtlinien in der Kategorie »Computerkonfiguration«

Betrachten wir zuerst die Richtlinien in der neuen Gruppenrichtlinie **OfficeXP-Computer** der Sub-OU **Benutzer** unterhalb der OU **Testfirma**. In der Kategorie **Computerkonfiguration · Administrative Vorlagen · Windows Installer** finden Sie einige Richtlinien, die das Verhalten bei der Installation von MSI-Dateien betreffen.



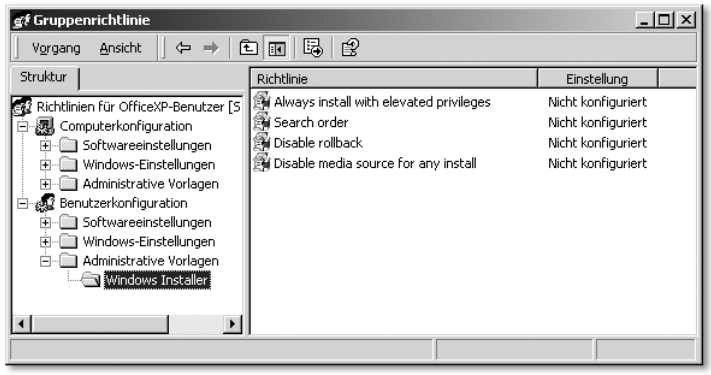
Exakt dieselben Richtlinien finden Sie aber in der Gruppendatei **SYSTEM.ADM**, die zum Lieferumfang von Windows XP (bzw. Windows Server 2003) gehört, und die wir in **XP-SYSTEM.ADM** umbenannt hatten, mit dem Unterschied, dass in der deutschen Fassung von Windows XP die Richtlinien nicht nur eingedeutscht sind, sondern auch noch Beschreibungen haben. Öffnen Sie zur Kontrolle einmal die Gruppenrichtlinie **XP-Standard** und dort **Computerkonfiguration · Administrative Vorgaben · Windows-Komponenten · Windows Installer.**



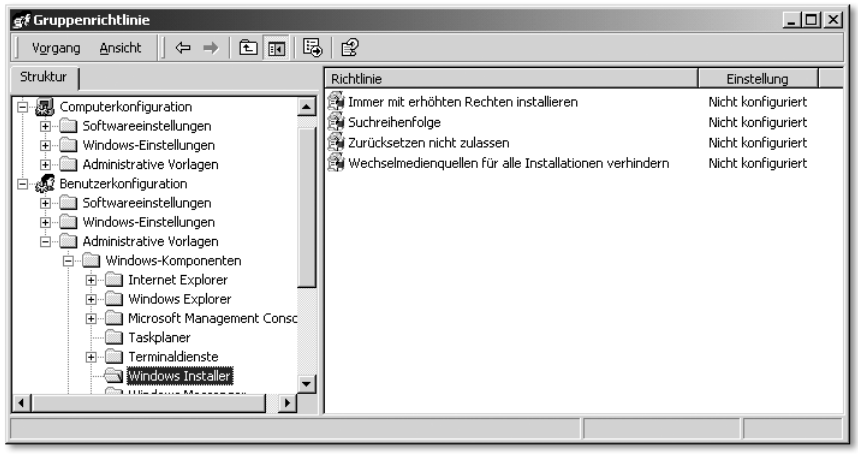
Diese Kategorie bietet dieselben Richtlinien wie die Datei **INSTLR11.ADM**, bis auf zwei weitere Richtlinien, nämlich **Benutzerinstallationen nicht zulassen** und **Erstellung von Systemwiederherstellungsprüfpunkten deaktivieren**. Wir können also festhalten, dass die neue ADM-Datei **INSTLR11.ADM** des Office XP Resource Kits eine weitere Kategorie namens **Windows Installer**

direkt unter **Computerkonfiguration · Administrative Vorlagen** hinzufügt, die es bereits eine Kategorie tiefer, nämlich unter **Computerkonfiguration · Administrative Vorlagen · Windows-Komponenten** gibt, wobei die bereits vorhandene Kategorie sogar zwei Richtlinien mehr bietet. Doppelt gemoppelt hält aber nicht unbedingt besser, sondern führt in der Informationstechnologie bekannter Weise zu Datenredundanzen und schnell zu Dateninkonsistenzen!

Die Vorlagedatei **INSTLR11.ADM** fügt aber nicht nur unter **Computerkonfiguration · Administrative Vorlagen** eine weitere Kategorie hinzu, sondern auch unter **Benutzerkonfiguration · Administrative Vorlagen.**



Doch auch die hier verfügbaren Richtlinien sind bereits in der Vorlagedatei **SYSTEM.ADM** von Windows XP vorhanden:



Warum liefert also Microsoft mit dem Office XP Resource Kit eine ADM-Datei namens **INSTLR11.ADM** mit Erstellungsdatum 06.06.2000 aus, die spätestens

durch die zum Lieferumfang von Windows XP gehörende **SYSTEM.ADM** obsolet geworden ist? Gab es die durch die **INSTLR11.ADM** hinzukommenden Richtlinien noch nicht unter Windows 2000? Um das zu überprüfen, können Sie in einer beliebigen OU eine neue Gruppenrichtlinie temporär erstellen und von den standardmäßig geladenen Vorlagedateien **conf**, **inetres** und **system** die Vorlagen **conf** und **inetres** entfernen. Wenn Sie anschließend wieder unter **Computerkonfiguration · Administrative Vorlagen · Windows-Komponenten · Windows Installer** bzw. unter **Benutzerkonfiguration · Administrative Vorlagen · Windows-Komponenten · Windows Installer** die vorhandenen Richtlinien mit den Richtlinien der **INSTLR11.ADM** vergleichen, stellen Sie dasselbe fest. Zumindest ab dem Service Pack 3 zu Windows 2000 enthält bereits die zum Lieferumfang des Betriebssystems gehörende **SYSTEM.ADM** dieselben Richtlinien wie die **INSTLR11.ADM**. Jetzt wird auch klar, warum die Datei **INSTLR11.ADM** ein Erstellungsdatum 20.06.2000 hat, während die anderen Vorlagedateien aus dem Office XP Resource Kit ein viel späteres Erstellungsdatum haben.

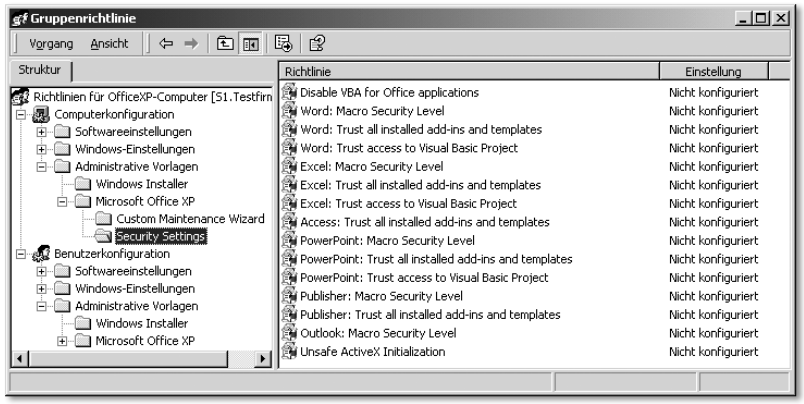
Der Schluss aus diesen Untersuchungen

Sie benötigen die Vorlagedatei **INSTLR11.ADM** aus dem Office XP Resource Kit nicht, weil alle von ihr bereitgestellten Richtlinien bereits von der Windows XP-Vorlagedatei **SYSTEM.ADM** mitgeliefert werden, dazu noch in deutscher Sprache und jeweils mit einer Beschreibung der Funktion dieser Richtlinie.

Entladen Sie also die Vorlage **INSTLR11** wieder aus den beiden zum Test eingerichteten Gruppenrichtlinien **OfficeXP-Computer** und **OfficeXP-Benutzer**. Danach löschen Sie außerdem die in das Verzeichnis **c:\winnt\inf** übernommene Datei **INSTLR11.ADM**, damit Sie gar nicht mehr in Versuchung kommen, diese Vorlagedatei in irgendeine Gruppenrichtlinie hinzuzuladen.

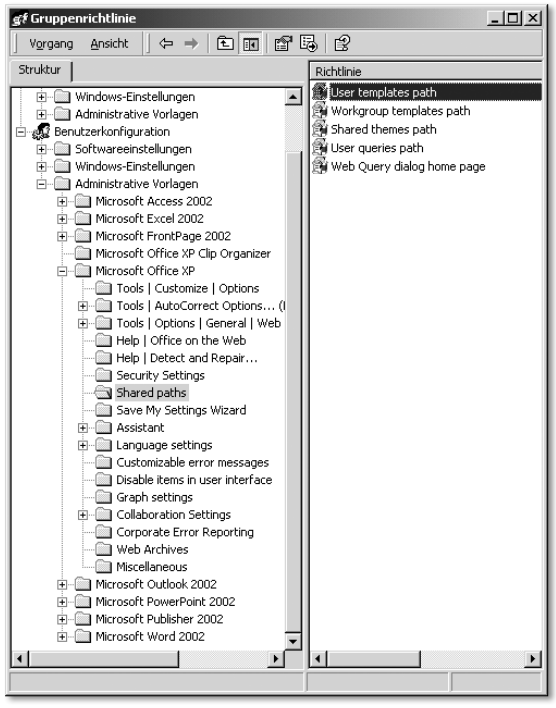
Mit den Richtlinien unter Microsoft Office XP – Custom Maintenance Wizard sollten Sie sich erst später befassen, wenn Sie sich das Tool **Custom Maintenance Wizard** aus dem Office Resource Kit angesehen haben und es einsetzen wollen. Mit diesem Tool kann eine CMW-Datei erstellt werden, um ein bereits ausgerolltes Office XP zu aktualisieren.

Mit den Richtlinien der Kategorie **Security Settings** können Sie die Makro-Sicherheit definieren und anderen Sicherheitslücken, die sich aus der Nutzung von Visual Basic for Applications (VBA) oder ActiveX-Controls ergeben, bei Bedarf zu Leibe rücken.



14.5 Office XP-Richtlinien in der Kategorie »Benutzerkonfiguration«

Sehen wir uns also jetzt die Office XP-Richtlinien an, die in der Kategorie **Benutzerkonfiguration · Administrative Vorlagen** hinzukommen. Dazu öffnen Sie in der Sub-OU **Benutzer** unterhalb der OU **Testfirma** die Richtlinie **OfficeXP-Benutzer**.



Suchen Sie unter www.google.de nach den Begriffen »keyfinder«, »OEM Preinstallation Kit« oder »Preinstallation Office XP«. Unter http://members.microsoft.com/partner/products/windows/windowsxp/Windows_XP_Tools_e.aspx finden Sie den Artikel »Windows XP Preinstallation Tools and Documentation« und unter http://members.microsoft.com/partner/products/windows/windowsxp/Preinstallation_Checklist.aspx eine Checkliste zur Vorinstallation von Windows XP.

Es kann für Sie auch sehr hilfreich sein, das Microsoft Action Pack zu abonnieren oder zumindest einen Blick hineinzuwerfen. Informationen zum Abonnement, das sich an Händler richtet, finden Sie über das Internet.

16.7 Welche Anwendungen gehören in ein Abbild, welche Anwendungen sollten nachinstalliert werden?

Mittels RIS, RIPrep oder Tools von Drittherstellern können Sie Abbilder von einem Computer erzeugen, auf dem das Betriebssystem und Standardanwendungen musterhaft installiert wurden. Dass die neueste Version von Microsoft Office sowie der Acrobat Reader in dieses Abbild aufgenommen werden, scheint selbstverständlich zu sein. Sicherlich wird es in Ihrem Unternehmen weitere Anwendungen geben, die auf dem Mustercomputer eingespielt und konfiguriert werden, bevor dann ein Abbild von diesem Computer erstellt wird, um es anschließend auf vielen Computern mit derselben HAL zu verteilen. Zu diesen Anwendungen wird vielleicht eine kaufmännische Anwendung wie z.B. die neueste Version von KHK SAGE oder des SAP Clients (SAPGUI) gehören, wahrscheinlich auch ein Virenscanner. Doch schon beim Virenscanner stellt sich die Frage, ob er in das Abbild eingehen oder über einen Software-Verteilmechanismus später dynamisch nachinstalliert werden soll.

Unbeaufsichtigte Installation von Anwendungen, die mit dem InstallShield kompiliert wurden

Der Acrobat Reader 5.x wird wie viele andere Anwendungen als sich selbst installierende EXE-Datei geliefert, z.B. mit der Bezeichnung **AcroReader51_DEU_Full.exe** bzw. **AdbeRdr60_deu_full.exe**. Die Installationsroutine wurde mit dem Programm **InstallShield** erstellt. Unter www.installshield.com finden Sie nähere Informationen zum **InstallShield** und Demoversionen. Unter http://support.installshield.com/kb/view.asp?articleid=q102394 finden Sie den Artikel »INFO: Setup.exe and Command Line Parameters«. Er listet auf, mit welchen Parametern die **Setup.exe** einer mit dem InstallShield erstellte Installationsroutine gestartet werden kann. Diese Parameter können Sie nutzen, um

als exe-Dateien gepackte Anwendungen zu entpacken und die entpackte Datei **setup.exe** bzw. die entpackte MSI-Datei über einen Parameter **/s** oder **/q** dann im »Quiet-Mode« zu starten. Auf diese Weise können diese Anwendungen oft unbeaufsichtigt verteilt werden. Die mühselige Neuerstellung eines MSI-Paketes entfällt damit. Weitere Informationen hierzu finden Sie auf der Buch-CD.

Wird eine Packer-Software benötigt?

Der Windows-Explorer von Windows XP Professional kann auch ZIP-Archive öffnen und erstellen. Dazu müssen Sie die Dateien markieren, die rechte Maustaste drücken und **Senden an ZIP-komprimierten Ordner** wählen. Folglich werden Sie wahrscheinlich kein spezielles Komprimierprogramm wie z.B. WINZIP für den Standardanwender benötigen. Denn die Lizenzkosten selbst für Shareware-Packer sind beträchtlich, wenn man mehrere hundert Lizenzen benötigt. Außerdem sind die Kosten für größere Festplatten derart gefallen, dass Sie kostengünstiger fahren, wenn Sie in weitere Serverplatten mit größerer Kapazität investieren, als wenn Sie die Anwender auffordern, Dateibestände zu komprimieren.

Wenn es zu Engpässen auf dem Dateiserver kommt, können Sie bestimmte Verzeichnisse auf dem Server mit Windows 2000/2003 eigenen Mitteln komprimieren, z.B. das Softwarearchiv-Verzeichnis, die Gruppenablagen oder die Basisverzeichnisse der Anwender (Home Directories). Dazu klicken Sie ein Verzeichnis mit der rechten Maustaste an und wählen **Eigenschaften · Erweitert · Inhalt komprimieren**. Die Komprimierrate ist ähnlich der Komprimierrate gängiger Packer-Software, der Anwender sieht gar nicht, dass diese Datenbestände auf dem Server in gepackter Form vorliegen und der Performance-Verlust beim Öffnen der Dateien ist meiner Erfahrung nach nicht spürbar.

Testen Sie das selbst einmal durch, indem Sie von einem Verzeichnis mit Office-Dokumenten sowie installierbaren EXE-Dateien ein Duplikat erstellen und das Duplikat komprimieren. Öffnen Sie dann vom Windows XP-Client aus zuerst die Office-Dokumente im nicht komprimierten Verzeichnis und danach dieselben Dokumente im komprimierten Verzeichnis. Installieren Sie danach z.B. die **rp505deu.exe** (Acrobat Reader 5.05) einmal aus dem nicht komprimierten Verzeichnis und danach aus dem komprimierten Verzeichnis.

Es muss jedoch darauf hingewiesen werden, dass auf dem Sicherungsband die komprimierten Datenbestände des Servers nicht komprimiert gesichert werden. Mit der Komprimierfunktion können Sie also die Speicherkapazität des Dateiservers kostenlos erweitern, müssen jedoch eventuell die Kapazität des Backupsystems vergrößern, um das Mehr an Daten auf dem Server auch wegsichern zu können.

Sollte der Virenscanner in das Abbild eines Mustercomputers eingehen?

Die Beantwortung dieser Frage hängt von verschiedenen Faktoren ab. Wenn es einen Standard-Arbeitsplatz gibt, der nicht mit einem Diskettenlaufwerk oder CDROM- bzw. DVD-Laufwerk ausgestattet ist, auf dem nur ganz bestimmte Anwendungen laufen (z.B. ein Buchungssystem und ein Mailclient wie Outlook), wenn dieser Standard-Arbeitsplatz zudem durch Gruppenrichtlinien derart eingeschränkt ist, dass der Anwender keine anderen Anwendungen starten kann und die Ausführung von Makros oder VBA-Skripten ebenfalls durch Gruppenrichtlinien deaktiviert sind, wenn weiterhin alle veränderlichen Daten nur auf dem Server und nicht auf dem Client abgespeichert werden können und somit das Risiko sehr beschränkt ist, dass der Client durch Viren verseucht werden kann und damit ein wirklicher Datenverlust verbunden wäre, so wäre es zwecks Einsparung von Lizenzkosten denkbar, dass Sie nur die Server (sowohl die Dateiserver als auch die Mailserver) durch Antiviren-Software absichern, natürlich unter der Prämisse, dass Sie eine Firewall einsetzen und die Antiviren-Software auf den Servern regelmäßig aktualisiert werden. In diesem Fall würden Sie nur auf bestimmten Clients wie den Administrator-Computern Virenscanner installieren und könnten damit unter Umständen viel Geld sparen. Jedoch müssten Sie dann in der Lage sein, bei Verdacht, dass sich doch ein Virus auf einem Client eingeschlichen hat, unverzüglich einen Virenscanner vom Software-Archiv nachzuinstallieren, um diesem Verdacht nachzugehen.

Diese Möglichkeit, Lizenzkosten für Antiviren-Software einzusparen, muss ich jedoch gleich wieder relativieren. Auch die Hersteller von Antiviren-Software sind auf die Schliche gekommen, dass Kunden auf die Idee kommen könnten, nur noch die Server gegen Viren abzusichern, indem z.B. im Extremfall nur noch Terminalserver-Technologie eingesetzt wird. Es ist prinzipiell möglich, z.B. Office XP auf einem Terminalserver zu installieren. Dann läuft Office XP nicht mehr im Hauptspeicher von vielen Clients ab, sondern im Hauptspeicher des Servers. Folglich könnte bei strikter Verwendung der Terminalserver-Technologie die Gefahr der Virenverseuchung von Clients theoretisch ausgeschaltet werden.

Große Hersteller von Antiviren-Software wie NAI (McAfee Total Virus Defense Suite), Symantec (AntiVirus Enterprise Edition) oder Sybari (Antigen for Exchange) haben diese Lizenzlücke jedoch gestopft. Die benötigte Lizenzanzahl richtet sich nach der Anzahl der am Server angeschlossenen Clients (bzw. Terminalclients) bzw. der Exchange-Postfächer und nicht nur nach der Anzahl der Server, auf denen die Antiviren-Software installiert ist. So verhält es sich,

nebenbei bemerkt, übrigens auch bei der Anzahl von benötigten Microsoft Office-Lizenzen.

Letztendlich ist aber für die Beantwortung der Eingangsfrage auch entscheidend, wie oft die so genannte »Engine« des Antivirenprodukts aktualisiert wird. Während die Antivirendateien oft schnell und ohne großen Aufwand über einen vom Hersteller für Netzwerke bereitgestellten Mechanismus auf die angeschlossenen Clients verteilt werden können, ist die Verteilung einer neuen Engine oft komplizierter und belastet unter Umständen die Leitungen intensiver.

Würde der Hersteller der Antiviren-Software in relativ kleinen Zeitabständen die Engine verändern, so wären die erstellten Abbilder schnell überaltert, wenn sie die Antiviren-Software enthalten würden. Folglich müssten die Abbilder in kurzen Zeitabständen überarbeitet werden. Stellt der Hersteller einen guten Mechanismus bereit, um ein komplettes Antiviren-Produkt (Engine und Antiviren-Dateien) über das Netzwerk zu verteilen, so macht es wahrscheinlich mehr Sinn, die Antiviren-Software nicht in das Abbild aufzunehmen, sondern separat über diesen Mechanismus hinzuzuinstallieren. Aber auch über die in Kapitel 10 »Das Loginskript« gezeigten Mechanismen oder über die Gruppenrichtlinie **Computerkonfiguration · Softwareeinstellungen · Softwareinstallation** ist es wahrscheinlich möglich, eine Antiviren-Software und deren Updates nachträglich zu verteilen.

Mein Rat: Nehmen Sie eine Antiviren-Software nach Möglichkeit nicht in die Abbilder auf, sondern suchen Sie nach einer Möglichkeit, Antiviren-Software und deren Updates dynamisch hinzuzuinstallieren. Die »Lebensdauer« der von Ihnen erstellten Abbilder steigt dadurch. Die Abbilder müssen nicht so oft überarbeitet werden.

Sollte der Client einer kaufmännischen Anwendung in das Abbild eines Mustercomputers eingehen?

Auch die Beantwortung dieser Frage hängt von verschiedenen Faktoren ab:

- Wird die kaufmännische Anwendung auf der Mehrheit der Clients benötigt, oder nur auf bestimmten Arbeitsplätzen?
- Wie schnell ändern sich die vom Hersteller aufgrund von aufgetretenen Programmfehlern veröffentlichten Release-Stände?
- Stellt der Hersteller einen eigenen brauchbaren Mechanismus zur Verfügung, um das Frontend des Produkts auf den Clients zu verteilen?
- Wird das Produkt pro installiertes Frontend lizenziert oder pro Zugriff auf die Serverdatenbank?

Versuchen wir, diese Fragen am Beispiel des SAP Frontends SAPGUI zu erörtern. SAP hat ein eigenes Benutzermanagement. Der Anwender von SAP muss sich also mit einer separaten Kennung und einem separaten Passwort am SAP-Server anmelden. Auch hier gibt es eine neue Entwicklung: Es ist zukünftig möglich, SAP so in das Microsoft Active Directory zu integrieren, dass sich der Anwender mit seiner Domänenkennung und seinem Domänenpasswort auch an der SAP-Datenbank anmeldet. Die getrennte Benutzerverwaltung von SAP fällt bei Ausnutzung dieser Möglichkeit weg.

SAP berechnet neuerdings die Anzahl der benötigten Lizenzen nicht mehr nach der Anzahl der Clients, auf denen der SAPGUI installiert ist. Sie könnten also zu dem Schluss kommen, dass es sinnvoll ist, das Frontend SAPGUI über ein Abbild auf allen Arbeitsplätzen zu verteilen, auch auf den Computern, an denen nicht mit SAP gearbeitet wird. Als Alternative müssten Sie sonst je HAL ein Abbild mit und ohne SAPGUI installieren – und die Pflege der Abbilder steigt ja proportional zur Anzahl der benötigten Abbilder.

Allerdings tauchten in der Vergangenheit bei neuen Release-Versionen des Frontends SAPGUI oft Fehler auf, und innerhalb kurzer Zeit verschickte SAP dann neue CDs mit fehlerbereinigten Versionen. Integrieren Sie die heute aktuelle Version 6.20 des Frontends SAPGUI in die Client-Abbilder und verteilen diese auf viele Computer, so kommt mit großer Wahrscheinlichkeit nach kurzer Zeit eine fehlerbereinigte neue Version auf den Markt. Sofort wären die Abbilder überaltert und sollten nicht auf weitere Computer aufgespielt werden, da Updates des SAP Frontends zumindest in der Vergangenheit nicht einfach eingespielt werden konnten, sondern eine vorangehende komplette Deinstallation der alten Version verlangten.

SAP liefert aber inzwischen mit seinen SAPGUI-CDs eine Methode aus, mit der die Art und Weise, wie und mit welchen Komponenten das Frontend verteilt werden soll, vorkonfiguriert werden kann. Mit dieser Methode kann dann eine Installation ohne Benutzereingaben im unbeaufsichtigten Modus ablaufen. Unter Verwendung der im Kapitel »Das Loginskript« gezeigten Möglichkeiten (Installation in einem administrativen Kontext starten) oder mittels der Gruppenrichtlinie **Computerkonfiguration · Softwareeinstellungen · Softwareinstallation** sollte es dann möglich sein, das jeweils aktuelle SAP Frontend separat zu verteilen. Das sind zu bedenkende Argumente, die zu der Entscheidung führen können, das SAP Frontend SAPGUI nicht in die Standard-Images aufzunehmen. Und diese Argumente werden wahrscheinlich auch auf andere kaufmännische Softwareprodukte zutreffen.

16.8 Welche Anwendungen können über Gruppenrichtlinien installiert werden?

Ist nun auch der Acrobat Reader oder eine andere Anwendung über eine Gruppenrichtlinie installierbar? Ja, immer dann, wenn der Hersteller eine MSI-Datei mitliefert, oder wenn Sie mit einem Tool eines Drittanbieters in der Lage sind, nachträglich eine MSI-Datei zu erstellen. Solch ein Tool finden Sie z.B. auf der Windows 2000 Server-CD im Verzeichnis **VALUEADD\3RDPARTY\MGMT\WINSTLE** als **WinINSTALL LE**. Diese Tools arbeiten alle nach derselben Methode: Sie starten das Tool und machen eine Ist-Aufnahme (Snapshot) des Clients. Danach starten Sie die Installation der betroffenen Anwendung. Nach Abschluss der Installation starten Sie die Anwendung und nehmen gewünschte Einstellungen vor. Danach starten Sie erneut das Tool und erzeugen erneut eine Ist-Aufnahme des Clients. Anschließend vergleicht das Tool die beiden Ist-Aufnahmen und erzeugt eine MSI-Datei, aus der alle Änderungen am System hervorgehen: neu hinzugekommene Verzeichnisse und Dateien, Änderungen an der Registrierdatenbank usw.

Zwei Tipps zu **WinINSTALL LE**: Zu WinINSTALL LE ist ein Patch erschienen, der einige Fehler behebt. (Download von http://seer.support.veritas.com/docs/229403.htm).

Installieren Sie das Tool nicht auf dem Client, auf dem Sie anschließend die eigentliche Anwendung installieren möchten. Konkret für unsere Testdomäne bedeutet das: Installieren Sie **WinINSTALL LE** auf dem Server **S1**, z.B. in der Freigabe **INSTALL**. Starten Sie das Tool anschließend auf dem Client, um die Ist-Aufnahme vor der Installation der neuen Anwendung durchzuführen. Danach installieren Sie die neue Anwendung und konfigurieren sie. Zuletzt starten Sie WinInstall erneut auf dem Client und erstellen auf dem Server die Differenzverzeichnisse und die MSI-Datei.

Doch Vorsicht: Diese Tools arbeiten nicht immer sauber! Oft enthalten die erzeugten MSI-Dateien nicht die hinzugekommenen Icons des Startmenüs oder es fehlen irgendwelche Dateien oder Einträge in INI-Dateien.

Für die Installation des Acrobat Readers konnte ich eine fehlerfrei funktionierende MSI-Datei erzeugen. Der Versuch, eine MSI-Datei für eine komplexere Anwendung wie den SAP-Client zu erstellen, führte zu großen Problemen und ich gab schließlich auf. Es erschien mir einfacher und zuverlässiger, für derartige Nachinstallationen die im Kapitel »Das Loginskript« verwendeten Methoden, speziell das selbst erstellte Tool **intel.exe** über ein Loginskript, einzuset-

zen. Mit dem Tool **Skriptit** kann man, wie in diesem Kapitel ebenfalls beschrieben, die Installation einer Anwendung weitgehend automatisieren. Die CD zum SAP-Client SAPGUI enthält außerdem selbst ein Tool, mit dem eine Clientinstallation vorkonfiguriert werden kann, sodass beim Ablauf der Installation keine Benutzereingaben mehr erwartet werden.

Es ist damit zu rechnen, dass viele Hersteller von Software dazu übergehen, MSI-Dateien mitzuliefern, da sich die von Microsoft promotete Installer-Technik mehr und mehr durchsetzt. Jedoch sollten Sie bei solchen Produkten auch überprüfen, ob der Hersteller ein Tool ähnlich dem Custom Installation Wizard aus dem Office Resource Kit mitliefert, damit Sie eine Transformationsdatei (MST-Datei) erzeugen können und somit die automatisierte Installation für Ihre Bedürfnisse anpassen können.

16.9 MSI-Pakete zuweisen oder veröffentlichen?

Noch ein Rat zur Installation von MSI-Paketen über Gruppenrichtlinien: Sie können nicht nur über **Computerkonfiguration · Softwareeinstellungen · Softwareinstallation** ein Installationspaket hinzufügen. Prinzipiell geht das auch über **Benutzerkonfiguration · Softwareeinstellungen · Softwareinstallation**. Fügen Sie ein MSI-Paket der Kategorie **Benutzerkonfiguration** hinzu, so können Sie das Paket wahlweise **zuweisen** oder **veröffentlichen**. Die Methode »Veröffentlichen« führt dazu, dass das Paket nicht sofort installiert wird. Entweder hat der Benutzer die Möglichkeit, über **Systemsteuerung · Software** die Anwendung endgültig zu installieren, oder aber der Anwender sieht bereits im Startmenü die Icons der neuen Anwendung, die Installation erfolgt jedoch erst, wenn der Anwender zum ersten Mal auf die Icons klickt.

Die Zuweisung von Installationspaketen an Benutzer oder Benutzer-Sicherheitsgruppen statt an Computer bzw. Computer-Sicherheitsgruppen ist lizenzrechtlich problematisch. Meldet sich ein Benutzer, dem ein Installationspaket über eine Gruppenrichtlinie zugeordnet wird, später an mehreren Computern an und startet das Icon der zugewiesenen Anwendung, so wird die Anwendung auf mehreren Computern installiert. Sie müssen in der Regel jedoch so viele Lizenzen einer Software erwerben, wie sie auf verschiedenen Computern installiert ist. Der Überblick darüber geht aber schnell verloren, wenn sich z. B. ein Mitarbeiter des Helpdesk, dem eine Anwendung zugeordnet wurde, an vielen Computern anmeldet. Solange Sie Installationspakete nur einer Organisationseinheit zuordnen, die Computer enthält, und nur über die Kategorie **Computerkonfiguration · Softwareeinstellungen · Softwareinstallation** diese Installationspakete zuordnen, müssen Sie auch nur die Anzahl der Computer

ler gelingt, die Preise aufgrund von fehlenden Alternativen zu diktieren. Doch von solchen Preisdiktaten ist dann nicht nur Ihr Unternehmen betroffen, sondern auch die Konkurrenz. Viel schlimmer als die Abhängigkeit von großen Herstellern ist aber eine andere Abhängigkeit, nämlich die Abhängigkeit von Einzelpersonen in Ihrem Unternehmen, den diese kann für Sie ruinös werden. Warum?

16.17 Abhängigkeit von Einzelpersonen vermeiden

Die Wahrscheinlichkeit, dass ein monopolistischer Hersteller wie Microsoft oder SAP in Konkurs geht und als Folge davon die IT-Infrastruktur Ihres Unternehmens in eine Sackgasse gerät, ist eher gering. Wenn jedoch die IT-Infrastruktur Ihres Unternehmens von dem Know-how eines oder weniger Systemadministratoren abhängt und nicht dokumentiert ist, so kann das fatale Folgen haben. Was geschieht, wenn diese Person von einem anderen Unternehmen von heute auf morgen abgeworben wird oder aber einen Unfall hat und nicht mehr verfügbar ist? Wie schnell kann sich ein neuer Mitarbeiter mit adäquater Ausbildung in die Strukturen des Netzwerkes einarbeiten. Welche Risiken bestehen, dass ein ehemaliger IT-Mitarbeiter nicht nur sein komplettes Know-how über das Netzwerk in ein Konkurrenzunternehmen transferiert und Sie »im Wald stehen lässt«, sondern auch noch Kundendaten, Preiskonditionen oder der Geheimhaltung unterliegende Datenbestände über neue Produkte, die noch in der Entwicklung sind, seinem neuen Arbeitgeber verfügbar macht?

Sich über die Abhängigkeit von großen Herstellern wie Microsoft oder SAP aufzuregen, ist mehr oder weniger verschwendete Energie. Sie als Systemadministrator und Entscheidungsträger in der IT-Abteilung können an diesen Abhängigkeiten kaum etwas verändern. Sehr wohl können Sie aber den Grad der Abhängigkeit von Einzelpersonen innerhalb Ihrer IT-Abteilung beeinflussen, indem Sie durch Qualitätsmanagement, einen hohen Grad der Standardisierung und eine ständig auf den neuesten Stand gebrachte Dokumentation des Netzwerks sicherstellen, dass jeder Mitarbeiter der IT-Abteilung ersetzbar bleibt.

16.18 Das Vier-Augen-Prinzip

Ein wichtiges Prinzip, dass Sie beherzigen sollten, ist das Vieraugen-Prinzip. Es sollte natürlich selbstverständlich sein, dass alle wichtigen Passwörter für den Fall, dass ein Systemadministrator ausfällt, in einem versiegelten Briefumschlag im Tresor des Unternehmens hinterlegt werden. Ein Mitarbeiter des Qualitätsmanagements muss in regelmäßigen Abständen kontrollieren, ob diese notier-

ten Passwörter wirklich funktionieren, der Inhalt des versiegelten Briefumschlags also ständig aktualisieren.

In Gesamtstrukturen, die aus einer Stammdomäne und mehreren Subdomänen bestehen, werden die Domänenadministratoren der Subdomänen eventuell befürchten, dass die Organisationsadministratoren und Schemaadministratoren der Stammdomäne ihre besondere Machtposition ausnutzen könnten und in den Subdomänen unkontrollierte Manipulationen vornehmen.

Die Organisations-Admins (Enterprise-Admins) haben folgende besonderen Rechte:

Nur Sie können den ersten Domänencontroller einer neuen Subdomäne einrichten und den letzten Domänencontroller einer Subdomäne löschen. Das heißt, nur die Organisations-Admins können in der Gesamtstruktur weitere Domänen einrichten und wieder löschen.

Nur die Organisations-Admins können neue Standorte sowie Standortverknüpfungen erstellen und den Standorten IP-Adressbereiche zuweisen. Nach der Einrichtung eines neuen Standortes können Sie die Administration dieses Standortes an andere Administratoren delegieren.

Die Gruppe Organisations-Admins wird bei der Einrichtung einer neuen Subdomäne automatisch in die Gruppe der Domänen-Admins eingetragen. Sie können aber aus dieser Gruppe entfernt und dann temporär wieder eingefügt werden, wenn z.B. unterhalb der Subdomäne eine weitere Subdomäne erstellt werden soll, denn auch das können nur die Organisations-Admins und nicht die Domänen-Admins.

Um zu verhindern, dass die Organisationsadministratoren zu viel ungewünschten Einfluss erhalten, gibt es aber nicht nur technische, sondern auch organisatorische Maßnahmen. Sie könnten zur Einhaltung eines schriftlichen Betriebskonzepts per Unterschrift angehalten werden, mit dem Hinweis, dass Zuwiderhandlungen mit disziplinarischen Maßnahmen geahndet werden. In diesem Betriebskonzept könnte schriftlich fixiert werden, dass Interaktionen nach Einrichtung der Subdomänen nur mit ausdrücklicher Genehmigung der dezentralen Domänenadministratoren zulässig sind und dann nur nach dem Vier-Augen-Prinzip erfolgen dürfen. Die Kennungen des Organisationsadministrators als auch des Schemaadministrators könnten z.B. aus einem 12-stelligen Passwort bestehen, dessen ersten 6 Stellen nur einem von zwei Administratoren und die zweiten 6 Stellen nur dem anderen Administrator bekannt sind. Würden beide 6-stelligen Teilpassworte schriftlich in separaten und versiegelten Umschlägen in einem Tresor aufbewahrt, so wäre sichergestellt, dass ein Administrator allein keine Handlungen (speziell keine widerrechtlichen

Handlungen) vornehmen kann. Bei der Abwesenheit eines der Organisationsadministratoren kann jedoch ein Vertreter in den Besitz des Teilpasswortskommen, um zusammen mit dem anderen Organisationsadministrator die notwendigen Handlungen vorzunehmen.

Ebenso muss es für Schemaänderungen am Active Directory, die nur durch Schemaadministratoren durchgeführt werden können, eine organisatorische Regelung geben, denn Schemaänderungen betreffen alle Subdomänen und sind nicht revidierbar. Produkte, die eine Schemaerweiterung benötigen, müssen in einer Testumgebung auf Kompatibilität mit den anderen Produkten getestet werden und am Besten durch eine Kommission freigegeben werden, der ein Domänenadministrator jeder Subdomäne angehört.

16.19 Das KISS-Prinzip zur Vermeidung unnötiger Komplexität

Microsoft liefert mit seinen Serverprodukten eine Technologie, mit der äußerst komplexe IT-Strukturen aufgebaut werden können. Die Anzahl der verwaltbaren Objekte im Active Directory ist inzwischen so groß, dass kaum eine Organisation an Grenzen stößt, wenn sie beabsichtigt, alle Organisationseinheiten in einer gemeinsamen Active Directory-Gesamtstruktur zu vereinigen. Doch auch das notwendige Know-how zur Beherrschung dieser Technologie ist immens gewachsen. Viele Wege führen nach Rom, wenn man sich in der konzeptionellen Planung der Gesamtstruktur befindet.

Man kann eine Organisation, die aus vielen Unterorganisationen besteht und räumlich dezentralisiert ist, auf mehrere Arten abbilden: durch mehrere Gesamtstrukturen, durch einen DNS-Namensraum, der unabhängig vom Active Directory ist, durch eine Stammdomäne mit vielen Subdomänen oder durch eine oder nur wenige Subdomänen, indem die ehemaligen selbstständigen NT 4.0-Domänen oder NetWare-Netze als Organisationseinheiten in einer Domäne zusammengeführt werden.

Sie können ein Meta-Directory einführen, um unterschiedliche Welten zusammenzuführen. Wenn Ihr Unternehmen international tätig ist, können Sie den Mitarbeitern nicht nur ein multilinguales Frontend-Betriebssystem und Office in der Landessprache zur Verfügung stellen, sondern auch auf den Servern die sprachlich lokalisierten Versionen einsetzten, oder aber zwecks Standardisierung und Reduzierung der Fehlerquellen und des Administrationsaufwandes sich zumindest bei den Serverprodukten auf eine Sprachversion einigen.

Sie können einen Wildwuchs von lokalen, globalen und universellen Sicherheits- oder Verteilergruppen erzeugen und dieses Gruppengebilde durch Ver-

18 Gruppen und Gruppenverschachtelung

Nur wenn sowohl eine Domäne als auch die Exchange-Organisation von Anfang an im einheitlichen Modus erstellt werden, kann die gewählte Gruppenstruktur durch die Beschränkung auf wenige Gruppenbereiche und durch eine Verschachtelung der Gruppen übersichtlich und leicht verwaltbar bleiben.

18.1 Gruppentypen und Gruppenbereiche

Unter Microsoft Active Directory gibt es die Gruppentypen **Sicherheitsgruppe** und **Verteilergruppe**. Sicherheitsgruppen können als Mitglieder Benutzer, externe Kontakte oder Computer haben, wobei Computer auch Server sein können. Sie können prinzipiell gemischte Sicherheitsgruppen erstellen, die z.B. als Mitglieder sowohl Benutzer als auch Computer haben. Einer Sicherheitsgruppe können Zugriffsrechte auf Dateien, Verzeichnisse, Freigaben und Netzwerkdrucker erteilt werden. Ebenso kann eine Sicherheitsgruppe berechtigt werden, bestimmte Objekttypen innerhalb einer bestimmten Organisationseinheit zu verwalten. Weiterhin ist es möglich, einer bestimmten Sicherheitsgruppe die Rechte **Lesen** und **Übernehmen** für eine Gruppenrichtlinie zu erteilen. Gruppen vom Typ **Sicherheit** können gleichzeitig als E-Mail-Verteilerlisten genutzt werden. Dazu klicken Sie die Gruppe mit der rechten Maustaste an und wählen **Exchange Aufgaben · E-Mail-Adresse erstellen**.

Verteilergruppen werden dann angelegt, wenn eine Gruppe von Benutzern über einen Exchange E-Mail-Verteiler adressiert werden können, jedoch keine Berechtigungen auf z.B. ein Gruppenverzeichnis erhalten soll. Auf einem Exchange Server können Sie Öffentliche Ordner erstellen. Wenn Sie die Zugriffsberechtigungen für einen öffentlichen Ordner verändern, indem Sie einer Verteilergruppe bestimmte Rechte geben, so wird die Verteilergruppe automatisch in eine Sicherheitsgruppe umgewandelt.

Probieren Sie das einmal aus: Erstellen Sie eine globale Verteilergruppe namens **Testverteiler** und erstellen Sie für diese Verteilergruppe eine Exchange E-Mail-Adresse, indem Sie die Verteilergruppe mit der rechten Maustaste anklicken, **Exchange Aufgaben** und anschließend **E-Mail-Adresse einrichten** wählen. Danach starten Sie Outlook, wechseln in **Öffentliche Ordner · Alle öffentlichen Ordner** und erstellen dort einen Testordner. Sie öffnen nun die Eigenschaften dieses Testordners, dort die Registerkarte **Berechtigungen**, fügen den neuen Verteiler **Testverteiler** hinzu und vergeben ihm Rechte. Danach verlassen Sie das Eigenschaftenfenster und schauen sich nun die Eigen-

schaften der ehemaligen Verteilergruppe **Testverteiler** an. Aus der Verteilergruppe ist eine Sicherheitsgruppe geworden.

Welche Konsequenzen hat das für Ihre Planung? Wenn aus Verteilergruppen spätestens dann, wenn man ihnen bestimmte Rechte auf einen öffentlichen Ordner des Exchange Servers zuweist, automatisch Sicherheitsgruppen werden, können Sie auch von vorneherein nur noch Sicherheitsgruppen anlegen. Damit bleibt Ihre Dokumentation sauber, denn die automatische Umwandlung einer Verteilergruppe in eine Sicherheitsgruppe werden Sie bewusst gar nicht mitbekommen, erst recht nicht, wenn Kollegen berechtigt sind, ab einer bestimmten Ordnerhierarchie eigene Öffentliche Ordner anzulegen und darauf Berechtigungen zu vergeben. Auch ist es unsinnig, eine Namenskonvention für Gruppen festzulegen, bei der in Sicherheitsgruppen und Verteilergruppen unterschieden wird, indem Sie z.B. jede Sicherheitsgruppe mit dem Buchstaben »S« und jede Verteilergruppe mit dem Buchstaben »V« beginnen würden. Spätestens nach einem Jahr Produktivbetrieb würden Sie wahrscheinlich feststellen, dass viele der Gruppen, deren Namen mit »V« beginnt, inzwischen zu Sicherheitsgruppen umgewandelt wurden.

Diese Gruppentypen haben jeweils die drei Gruppenbereiche **Lokale Domäne**, **Global** und **Universal**, wobei die Begriffe »universal« und »universell« in der Fachliteratur durcheinander verwendet werden. Im Snap-In **Active Directory-Benutzer und -Computer** heißen diese Gruppen **Universal**, gemeint ist aber, dass sie universell genutzt werden können. Auch ich benutze beide Begriffe in diesem Buch nebeneinander.

In der Fachliteratur werden nun diese drei Gruppen gegeneinander abgegrenzt. Dabei wird in der Regel ein Konzept zur Nutzung dieser Gruppenbereiche herangezogen, bei dem ein Mehrdomänenkonzept Pate steht und es wird darauf hingewiesen, dass dieses Konzept bei späteren Erweiterungen die größte Flexibilität bietet. Dieses Konzept schlägt folgende Vorgehensweise vor: Alle Benutzer, die auf eine bestimmte Ressource zugreifen sollen (z.B. auf bestimmte Netzdrucker oder ein bestimmtes Gruppenverzeichnis auf einem Dateiserver), sollen in einer globalen Gruppe zusammengefasst werden. Die passenden Rechte für die Ressource sollen jedoch nicht direkt dieser globalen Gruppe erteilt werden. Stattdessen soll eine lokale Gruppe erstellt werden, und die globale Gruppe soll als Mitglied in diese lokale Gruppe aufgenommen werden. Diese lokale Gruppe soll nun die passenden Rechte auf die Ressource erhalten.

Diese Vorgehensweise wird damit begründet, dass auf diese Weise auch Mitglieder einer anderen Domäne der Gesamtstruktur auf diese Ressource zugreifen können. Da globale Gruppen immer nur Mitglieder derselben Domäne,

lokale Gruppen jedoch auch globale Gruppen anderer Domänen aufnehmen können, kann auf diese Weise z.B. auf ein Verzeichnis **Projekt ABC** des Servers **S1.HansenVerlag.Testfirma.de** nicht nur jedem Mitglied der globalen Gruppe **Projekt ABC HansenVerlag** der Zugriff gewährt werden, sondern auch der globalen Gruppe **Projekt ABC BensonVerlag**, wenn die letztere zur Subdomäne **BensonVerlag.Testfirma.de** gehört und folglich nur Domänenbenutzer der Subdomäne **BensonVerlag** enthält.

Sie können und sollten vielleicht auch so vorgehen, wenn Ihre Gesamtstruktur aus politischen Gründen unbedingt eine Vielzahl von Subdomänen unter einer Stammdomäne vereint. Doch macht dies die Verwaltung bestimmt nicht gerade einfacher. Ein Grundprinzip bei der Einführung von Active Directory ist nämlich, dass Sie den Umbau ehemaliger Windows NT 4.0-Domänen und Netware-Netze nutzen sollten, um diese Komplexität zurückzuführen, indem ehemalige NT 4.0-Domänen unter Microsoft Active Directory in Organisationseinheiten umgewandelt werden und im Idealfall unter einer einzigen Domäne zusammengeführt werden. Organisationseinheiten sind nämlich später bei Umstrukturierungen viel flexibler als Subdomänen.

Außerdem kommt es in der Praxis oft nur ausnahmsweise vor, dass Mitarbeiter verschiedener Subdomänen auf dieselben Ressourcen zugreifen müssen. Handelt es sich hierbei um Ordner mit Dokumenten (z.B. Projektordner), so können Sie diesen Projektordner auch als öffentlichen Exchange-Ordner verfügbar machen. Eine Exchange-Organisation ist jedoch nicht an eine bestimmte Domäne gebunden. Sie können ein und dieselbe Exchange Organisation für alle Domänen einer Gesamtstruktur nutzen, ja müssen es sogar, da zumindest unter Windows 2000 Server und Exchange 2000 Server es nicht möglich ist, zwei Exchange Organisationen in einem Domänenwald parallel zu betreiben.

Altlasten aus Windows NT 4.0-Domänen

In Windows NT 4.0-Domänen gab es Beschränkungen, die es in einer Windows 2000/2003-Domäne zwar nicht mehr gibt, wenn diese im einheitlichen Modus betrieben wird. Dennoch wirken diese ehemaligen Restriktionen in der Literatur auch auf Active Directory zurück, wenn Empfehlungen ausgesprochen werden, welche Gruppenbereiche genutzt und wie diese Gruppen ineinander verschachtelt werden sollen. Lesen Sie deshalb auch dann den nachfolgenden Abschnitt, wenn Sie keine NT 4.0-Domänen migrieren müssen. Danach werden Sie verstehen, warum die in der Literatur ausgesprochenen Empfehlungen oft so konfus wirken, und dass diese Empfehlungen kritisch zu beurteilen sind.

Erinnern wir uns: Unter NT 4.0 gab es Primary Domain Controller (PDCs) und Backup Domänen Controller (BDCs), Einzeldomänen, Masterdomänen und Ressourcen-Domänen, mehrfache Master-Domänen, einfache und gegenseitige Vertrauensbeziehungen zwischen den Domänen. Eine einzelne Domäne durfte wegen der Beschränkung der SAM-Datenbank nicht mehr als 40.000 Konten haben, wobei dieser Maximalwert wohl eher theoretischer Natur war, weil eine SAM-Datenbank mit 40.000 Konten nicht nur wegen der Performance des Domänencontrollers erhebliche Schwierigkeiten bereitet hätte, sondern auch bei der Replikation zumindest über langsame WAN-Leitungen das Netzwerk lahm gelegt hätte. In größeren Organisationen wurden also viele Einzeldomänen angelegt, um nicht in Konflikt mit dieser Restriktion zu geraten. Diese Einzeldomänen mussten dann über Vertrauensstellungen manuell miteinander verwoben werden.

Es gab keine universellen Gruppen, sondern nur lokale und globale Gruppen. Lokale Gruppen wurden nur in der lokalen Kontendatenbank verwaltet, globale Gruppen jedoch in der Domänenkontenbank. Eine lokale Gruppe wurde z.B. für einen Mitgliedsserver erstellt, Rechte für diese lokale Gruppe konnte dann aber auch nur für Ressourcen auf diesem Mitgliedsserver vergeben werden. Lokale Gruppen konnten als Mitglieder zwar globale Gruppen derselben Domäne oder einer vertrauten Domäne aufnehmen, jedoch konnten die lokalen Gruppen nicht ineinander verschachtelt werden. Globale Gruppen wiederum konnten nur Benutzer oder Computer aufnehmen, jedoch keine anderen globalen Gruppen und auch keine lokalen Gruppen.

Solange Sie eine Windows 2000/2003-Domäne im gemischten Modus fahren, weil Sie alte Windows NT 4.0-Server integrieren müssen, gelten alle diese Restriktionen weiter. Erst nach der Umstellung in den einheitlichen Modus sind Sie endgültig davon befreit. Das gilt auch für einen Gemischtbetrieb von Exchange 2000 Servern und Exchange 5.5 Servern. Erst nach der Umstellung in den einheitlichen Modus gibt es keine Restriktionen mehr hinsichtlich der Verwendung der Gruppenbereiche und der Gruppenverschachtelung.

Sicherheitsgruppen im Active Directory

In Active Directory sieht die Sache ein wenig anders aus: Die Anzahl von Konten in einem Domänenwald ist faktisch unbeschränkt, ein Grund, möglichst wenig Domänen in der Gesamtstruktur anzulegen, sondern OUs zur Strukturierung zu nutzen.

Lokale Gruppen können ineinander verschachtelt werden, man spricht jetzt auch von **domänenlokalen Sicherheitsgruppen**, was nichts anderes bedeutet, als dass jetzt auch die lokalen Gruppen im Active Directory und nicht mehr

in der lokalen Sicherheitsdatenbank verwaltet werden. Das wiederum bedeutet, dass einer lokalen Gruppe nun Rechte für beliebige Ressourcen innerhalb der Domäne zugewiesen werden können, in der sie erstellt wurde. Die lokale Gruppe ist also nicht mehr an einen speziellen Server gebunden.

Ebenso können globale Gruppen einer Domäne ineinander verschachtelt werden. Im einheitlichen Modus kann die globale Gruppe ein Mitglied von globalen, lokalen oder universalen Gruppen in der gleichen Domäne sein. Eine globale Gruppe der Domänen x kann aber auch ein Mitglied von universalen oder lokalen Gruppen einer anderen Domäne y sein, wenn beide Domänen zu derselben Gesamtstruktur gehören. Eine globale Gruppe der Domäne x kann aber nicht ein Mitglied einer globalen Gruppe einer anderen Domäne sein.

Universale Gruppen werden zur Zusammenfassung von Gruppen aus unterschiedlichen Domänen zu einer administrativen Einheit verwendet. Eine Liste der Mitgliedschaften in universalen Gruppen wird im globalen Katalog verwaltet. Änderungen an den Daten, die im globalen Katalog gespeichert werden, werden zu jedem globalen Katalog in einer Gesamtstruktur repliziert. Indem die Verwendung universaler Gruppen minimiert wird, kann die Replikationsaktivität im Wesentlichen auf eine einzelne Domäne beschränkt werden.

Sollten Sie aus diesem Grunde aber die Anzahl der universellen Gruppen minimieren? Repliziert werden immer nur Änderungen auf Attributsebene, nicht aber das ganze Objekt. Wenn sich also die Telefonnummer oder der Nachname eines Benutzers ändert, so wird nur diese Attributsänderung über Domänengrenzen hinweg weitergegeben, es wird aber nicht das ganze Objekt mit all seinen Attributsinhalten erneut repliziert.

Sobald Ihre Gesamtstruktur steht und alle Benutzer angelegt und die Gruppenmitgliedschaften festgelegt wurden, nimmt der Replikationsverkehr drastisch ab. Es sei denn, Sie arbeiten in einer Organisation, in der eine hohe Personalfluktuation herrscht oder permanent umstrukturiert wird, sei es durch Firmenfusionen oder Firmenauflösungen, sei es durch sich ständig und in großer Anzahl sich ändernder Projektgruppen und Mitgliedschaften in temporären Projektgruppen.

Das Konzept, Benutzer nur in globale Gruppen aufzunehmen, diese globalen Gruppen wiederum zu Mitgliedern von lokalen Gruppen zu machen und nur den lokalen Gruppen Rechte zu Ressourcen zuzuweisen, führt damit zu einer unnötigen Komplexität, die eigentlich nur berechtigt ist, solange Sie sich in der Umbauphase von Windows NT 4.0-Domänen zu einem Active Directory befinden.

Haben Sie diese Altlasten nicht oder führen Sie statt einer Migration (Update von alten NT 4.0-Domänencontrollern auf Windows 2000 Server bzw. Windows 2003 Server) das neue System Active Directory parallel ein und ersetzen schlagartig, statt über die »sanfte Migration« ein lokales Netzwerk durch das Active Directory, so können Sie das neue System sofort im einheitlichen Modus fahren und alle Vorteile nutzen.

Ich rate Ihnen dazu, diesen Weg zu gehen. Oft sind die alten NT 4.0-Server vom Stand der Technik überaltert. Serverhardware verliert pro Jahr ungefähr 50 Prozent an Wert. Schon alleine deshalb sind der Aufwand und das Risiko, alte Windows NT 4.0-Server mühselig auf Windows 2000/2003 Server zu updaten, oft unakzeptabel. Sie können besser die alte Serverhardware für andere Zwecke weiterverwenden und parallel zur alten Windows 4.0-Domäne ein sauberes Active Directory auf neuer Serverhardware im einheitlichen Modus hochziehen, mit Testkennungen und Testgruppen durchprüfen und dann eine Abteilung nach der anderen schlagartig umstellen. Bei dieser Umstellung werden Sie dann auch die Workstations mit einem Image innerhalb kürzester Zeit auf das aktuelle Betriebssystem und die aktuelle Office-Version umstellen und dabei überalterte Client-Hardware aussondern.

Die Kenntnisse, die Ihre Mitarbeiter sich aneignen müssen, um die Besonderheiten eines Gemischtmodus von Active Directory und alter NT 4.0-Domänenlandschaft sowie einem Gemischtmodus von Exchange 2000 und Exchange 5.0/5.5 zu beherrschen, sind enorm. Der Gemischtbetrieb ist fehleranfällig.

Versuchen Sie darüber hinaus auch noch, Netware-Netze zu integrieren, so werden Sie mit großer Wahrscheinlichkeit irgendwo im Umstellungsprozess stecken bleiben und nie zu sauberen und überschaubaren Strukturen gelangen. Vor allem wird es Ihnen nicht gelingen, eine Dokumentation zu erstellen, die alle Zwischenschritte mit allen Besonderheiten darstellt und auf dem Weg zum einheitlichen Modus ständig mit gepflegt werden soll. Und denken Sie daran, dass auch die für die Verwaltung von Active Directory bestimmenden Elemente wie Gruppenrichtlinien, Organisationseinheiten, Zuweisung von Verwaltungsaufgaben über OUs für Server und Clients unter Windows NT 4.0 nicht wirken.

1. Beispiel: Einzeldomäne

Gibt es nur eine Domäne, die aus nur zwei Domänencontrollern **DC1** und **DC2** sowie weiteren Mitgliedsservern besteht, so sollten die Rollen wie folgt verteilt werden:

DC1: Schemamaster, DNS-Master und globaler Katalog

DC2: Infrastrukturmaster, RID-Master und PDC-Emulator

2. Beispiel: Domänenwald

Gibt es eine Stammdomäne **Testfirma.de** mit zwei Domänencontrollern **DC1** und **DC2** sowie zwei Subdomänen **SUB1.Testfirma.de** und **SUB2.Testfirma.de**, und bestehen die beiden Subdomänen aus jeweils 2 Domänencontrollern (**DC1SUB1**, **DC2SUB1**, **DC1SUB2** und **DC2SUB2**) und sonst nur Mitgliedsservern, so sollten die Rollen wie weiter unten angegeben:

Auf den beiden Domänencontrollern der Stammdomäne **Testfirma.de** werden die Rollen wie im ersten Beispiel verteilt:

DC1: Schemamaster, DNS-Master und globaler Katalog

DC2: Infrastrukturmaster, RID-Master und PDC-Emulator

Auf den Domänencontrollern **DC1SUB1** und **DC2SUB1** der Subdomänen **SUB1.Testfirma.de** werden die Rollen wie folgt verteilt:

DC1SUB1: Infrastrukturmaster, RID-Master und PDC-Emulator

DC2SUB1: globaler Katalog

Auf den Domänencontrollern **DC1SUB2** und **DC2SUB2** der Subdomänen **SUB2.Testfirma.de** werden die Rollen analog zur Subdomäne **SUB1.Testfirma.de** verteilt:

DC1SUB2: Infrastrukturmaster, RID-Master und PDC-Emulator

DC2SUB2: globaler Katalog

19.3 Die Verschiebung der Betriebsmaster-Rollen

Wenn ein Domänencontroller heruntergefahren wird, überträgt er nicht automatisch seine Betriebsmasterfunktionen an einen anderen Domänencontroller. Dies wäre auch nicht sinnvoll, da die Aufteilung der FSMO-Rollen auf die verschiedenen Domänencontroller ja aus verschiedenen Gründen geplant war und nicht einfach durch einen Automatismus des Betriebssystems geändert werden sollten. Solange ein Domänencontroller z. B. aus Wartungsgründen (Ausbau

der Hardware oder Austausch defekter Hardware-Komponenten) nur eine befristete Zeit vom Netz geht, müssen in der Regel die FSMO-Rollen nicht verschoben werden. Die FSMO-Rollen müssen jedoch bei der erstmaligen Einrichtung mehrerer Domänencontroller verteilt werden und dann neu zugeordnet werden, wenn ein Domänencontroller neu hinzukommt oder endgültig (gewollt oder ungewollt) ausfällt.

Die Vorgehensweise bei der Übertragung bzw. der Übernahme einer FSMO-Rolle wird im Artikel »223787 – Flexible Single Master Operation Transfer and Seizure Process« der Microsoft Knowledge Base beschrieben.

Die Routine DUMPFSMOS.CMD zum Anzeigen der Betriebsmasterfunktionen

Im Windows Server 2003 Resource Kit finden Sie die Routine **Dumpfsmos.cmd** (Dump FSMO Roles). Sie hat folgenden Inhalt:

```
@echo off
REM
REM Script to dump FSMO role owners on the server designated by %1
REM
if ""=="%1" goto usage
ntdsutil roles Connections "Connect to server %1" Quit "select
Operation Target" "List roles for connected server" Quit Quit Quit
goto done
:usage
@echo Please provide the name of a domain controller
@echo.
:done
```

Diese Routine zeigt die Betriebsmasterfunktionen (FSMO-Rollen) eines Domänencontrollers an. Der Befehl »dumpfsmos Server1« erzeugt z.B. folgendes Ergebnis, wenn alle FSMO-Rollen vom selben Domänencontroller Server1 ausgeführt werden:

ntdsutil: roles
fsmo maintenance: Connections
server connections: Connect to server Server1
Binding to Server1 ...
Connected to Server1 using credentials of locally logged on user.
server connections: Quit
fsmo maintenance: select Operation Target
select operation target: List roles for connected server

Server "Server1" knows about 5 roles
Schema - CN=NTDS Settings,CN=SERVER1,CN=Servers,CN=New-Site,CN=Sites,CN=Configuration,DC=contoso,DC=com
Domain - CN=NTDS Settings,CN=SERVER1,CN=Servers,CN=New-Site,CN=Sites,CN=Configuration,DC=contoso,DC=com
PDC - CN=NTDS Settings,CN=SERVER1,CN=Servers,CN=New-Site,CN=Sites,CN=Configuration,DC=contoso,DC=com
RID - CN=NTDS Settings,CN=SERVER1,CN=Servers,CN=New-Site,CN=Sites,CN=Configuration,DC=contoso,DC=com
Infrastructure - CN=NTDS Settings,CN=SERVER1,CN=NewSite,CN=Sites,CN=Configuration,DC=contoso,DC=com
select operation target: Quit
fsmo maintenance: Quit
ntdsutil: Quit
Disconnecting from Server1...

Wann sollten Betriebsmasterfunktionen übertragen werden?

Im Artikel »Professor Windows – March 2002 – Best Practise for Active Directory Design and Deployment« (www.microsoft.com/technet/colums/profwin) finden Sie folgende Hinweise zum Ausfall von Domänencontrollern mit Betriebsmasterfunktionen:

> *»A few words on Flexible Single Master Operation (FSMO) roles offline scenarios Having the Schema, Domain Naming master and Infrastructure master offline for a short time does not affect the Directory Service. Essentially, the RID Master is also non-critical for a short period of time, unless you're planning bulk-operations (migrations) at the time of the outage. The RID master should be brought back on-line in a few hours, just to be on the safe side. The exception is the PDC Emulator role, which should be online always. For any of the other FSMO roles, transfer the role(s) to another server only when the role is needed urgently, and while perfectly understanding that the original server that held that role up till now is NOT coming back online into your network without a re-install.«*

Das Tool NTDSUTIL zum Übertragen oder Übernehmen von Betriebsmasterfunktionen

Die Betriebsmasterfunktionen können zwischen den Domänencontrollern über das Befehlszeilenprogramm **NTDSUTIL** verschoben werden.

So übertragen Sie die Funktion des Schemamasters

Die Übertragung der Funktion Schemamaster vom Domänencontroller **DC1** aus auf den Domänencontroller **DC2 m**it dem Tool **NTDSUTIL** läuft wie folgt ab:

1. Klicken Sie auf **Start** und dann auf **Ausführen**, und geben Sie **cmd** ein.
2. Sie geben den Befehl **ntdsutil** ein.
3. Es erscheint eine Meldung **ntdsutil**: Geben Sie **roles** ein.
4. Es erscheint eine Meldung **FSMO-Wartung**: Geben Sie **connections** ein.
5. Hinter der Meldung **Serververbindungen**: Geben Sie **connect to server dc2** ein.
6. Geben Sie **quit** ein.
7. Der nächste Befehl lautet **transfer schema master**.
8. Die Rollenübertragung muss in einem sich öffnenden Fenster **Transfer Confirmation Dialog: Are you sure you want server dc2.Testfirma.de to transfer the schema master for the enterprise?** durch Klicken auf die Schaltfläche **Yes** bestätigt werden.

Fällt der Domänencontroller **DC1** aus, so kann auch eine Rollenübernahme vom zweiten Domänencontroller **DC2** aus eingeleitet werden. Die Abfolge der Befehle ist ähnlich der Abfolge der Befehle bei der Übertragung der Rolle vom **DC1** aus. Jedoch muss statt des Befehls **transfer schema master** dann der Befehl **seize schema master** eingegeben werden. Es öffnet sich dann ein Fenster **Role Seizure Confirmation**, in dem die Rollenübernahme durch Anklicken der Schaltfläche **Yes** bestätigt werden muss.

So übernehmen Sie die Funktion des Schemamasters

1. Klicken Sie auf **Start** und dann auf **Ausführen**, und geben Sie **cmd** ein.
2. Geben Sie an der Eingabeaufforderung **ntdsutil** ein.
3. Geben Sie an der Eingabeaufforderung **ntdsutil** den Befehl **roles** ein.
4. Geben Sie an der Eingabeaufforderung **FSMO-Wartung** den Befehl **connections** ein.
5. Geben Sie an der Eingabeaufforderung **Serververbindungen** den Befehl **connect to server**, gefolgt von einem vollqualifizierten Domänennamen, ein.
6. Geben Sie an der Eingabeaufforderung **Serververbindungen** den Befehl **quit** ein.
7. Geben Sie an der Eingabeaufforderung **FSMO-Wartung** den Befehl

8. **seize schema master** ein.
9. Geben Sie an der Eingabeaufforderung **FSMO-Wartung** den Befehl **quit** ein.
10. Geben Sie an der Eingabeaufforderung **ntdsutil** den Befehl **quit** ein.
11. Vorsicht! Die Übernahme des Schemamasters ist ein drastischer Schritt, der nur in Betracht gezogen werden sollte, wenn ein neuerlicher Betrieb des aktuellen Betriebsmasters vollständig ausgeschlossen wird.

So übernehmen Sie die RID-Masterfunktion

Verfahren Sie wie unter »So übernehmen Sie die Funktion des Schemamasters«. Geben Sie jedoch im Punkt 7 den Befehl **seize RID master** ein.

Vorsicht! Die Übernahme der RID-Masterfunktion ist ein drastischer Schritt, der nur in Betracht gezogen werden sollte, wenn ein neuerlicher Betrieb des aktuellen Betriebsmasters vollständig ausgeschlossen wird.

Vor der Übernahme des RID-Masters können Sie mit dem Programm **Repadmin** aus den Active Directory-Supporttools prüfen, ob der neue Betriebsmaster Aktualisierungen des vorherigen Masters empfangen hat. Entfernen Sie dann den aktuellen Betriebsmaster aus dem Netzwerk.

So übernehmen Sie die DNS-Masterfunktion

Verfahren Sie wie unter »So übernehmen Sie die Funktion des Schemamasters«. Geben Sie jedoch im Punkt 7 den Befehl **seize domain naming master** ein.

Vorsicht! Die Übernahme der DNS-Masterfunktion ist ein drastischer Schritt, der nur in Betracht gezogen werden sollte, wenn ein neuerlicher Betrieb des aktuellen Betriebsmasters vollständig ausgeschlossen wird.

So übernehmen Sie die Funktion des Infrastrukturmasters

Verfahren Sie wie unter »So übernehmen Sie die Funktion des Schemamasters«. Geben Sie jedoch im Punkt 7 den Befehl **seize infrastructure master** ein.

Anmerkung: Wenn der ursprüngliche Infrastrukturmaster wieder in Betrieb genommen wird, können Sie die Funktion wieder auf den ursprünglichen Domänencontroller übertragen.

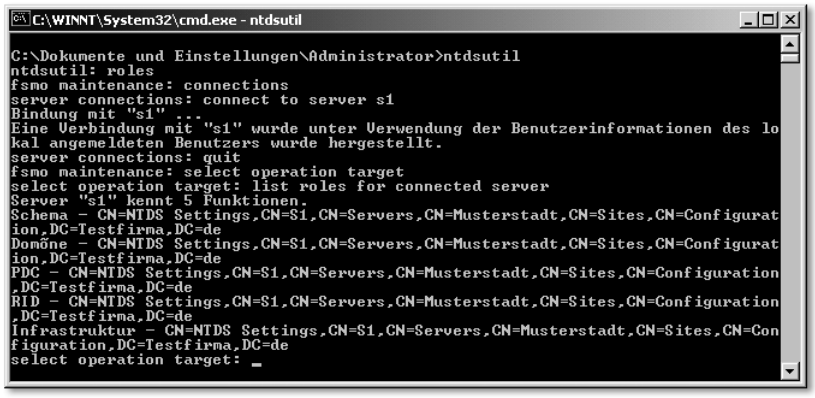
So übernehmen Sie die PDC-Emulationsfunktion

Verfahren Sie wie unter »So übernehmen Sie die Funktion des Schemamasters«. Geben Sie jedoch im Punkt 7 den Befehl **seize PDC** ein.

Anmerkung: Wenn der ursprüngliche PDC-Emulator wieder in Betrieb genommen wird, können Sie die Funktion wieder auf den ursprünglichen Domänencontroller übertragen.

Die FSMO-Rollen eines Servers anzeigen

Das Tool **NTDSUTIL** ermöglicht auch das Anzeigen von Betriebsmaster-Rollen. Die Eingabe der Befehle ist weitgehend identisch, jedoch muss statt des Befehls **transfer schema master** bzw. **seize schema master** der Befehl **select operation target** und danach der Befehl **list roles for connected server** eingegeben werden. Die Ausgabe kann wie folgt aussehen:

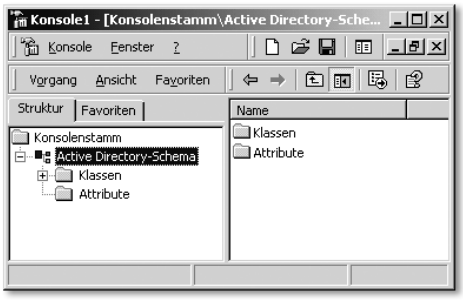


Snap-Ins zur grafischen Anzeige und Übertragung der Betriebsmasterfunktionen

Neben dem Tool **NTDSUTIL** können Sie auch Snap-Ins benutzen, um die FSMO-Rollen grafisch zu managen. Zum Anzeigen der Server mit domänenspezifischen Betriebsmasterrollen starten Sie **Active Directory-Benutzer und -Computer**, klicken den Domänennamen mit der rechten Maustaste an und wählen **Betriebsmaster** aus. Sie sehen drei Register für die Rollen RID, PDC und Infrastruktur und können die Rollen über die Schaltfläche **Ändern** verschieben.

Zuvor muss jedoch eine Verbindung zum Zieldomänencontroller hergestellt werden. Auch dazu klicken Sie den Domänennamen mit der rechten Maustaste an und wählen den Befehl **Verbindung mit Domänencontroller herstellen**.

Zum Anzeigen des Schemamasters muss das Snap-In **Active Directory-Schema** gestartet werden. Aus Sicherheitsgründen wird dieses Snap-In jedoch nicht unter **Programme · Verwaltung** angezeigt. Sie müssen zuerst den Befehl **mmc** eingeben, im Menü **Konsole** die Option **Snap-In hinzufügen/entfernen** wählen, erneut **Hinzufügen** wählen und aus der Liste der verfügbaren Snap-Ins das Snap-In **Active Directory-Schema** wählen.



Wenn Sie in der neuen Konsole **Active Directory-Schema** mit der rechten Maustaste anklicken, können Sie die Option **Betriebsmaster** wählen. Im Fenster **Schemamaster ändern** ist auch beim ersten Domänencontroller einer Domäne die Option **Schema kann auf diesem Domänencontroller geändert werden** nicht standardmäßig aktiviert! Über die Schaltfläche **Ändern** können Sie aber auch die Schemamasterrolle verschieben.

Um den DNS-Master anzuzeigen bzw. die Rolle zu verschieben, starten Sie das Snap-In **Active Directory-Domänen und -Vertrauensstellungen**, klicken

names. For example, NTServer_1 becomes NTServer-1, leading to failure of name resolution of a name that may, in fact, be recorded in the DNS files.«

»Align the Lease and Refresh Periods for DHCP and WINS

When you configure a network to use both DHCP and WINS, set the DHCP lease period to be roughly equal to or greater than the WINS renewal period. This prevents a situation in which the WINS server fails to notice that a DHCP client releases a DHCP-assigned IP address; the client cannot send a WINS renewal request if the client fails to renew its IP address. If another computer is assigned that IP address before the WINS server notes the change, the WINS server mistakenly directs requests for the address to the new client.«

20.4 Zeitserver

Der erste Domänencontroller, der in einer neuen Gesamtstruktur von Domänen erstellt wird, fungiert standardmäßig als Zeitserver für die anderen Server, während sich Clients mit Windows XP Professional automatisch bei der Anmeldung an einem Domänencontroller die aktuelle Zeit von diesem Domänencontroller abholen. Der Artikel »216734 – How to Configure an Authoritative Time Server in Windows 2000« in der Microsoft Knowledge Base erklärt, wie die Clients und die Server in einem Active Directory-Forest die interne Zeit synchronisieren:

»Windows-based computers use the following hierarchy by default:

All client desktop computers nominate the authenticating domain controller as their in-bound time partner.

All member servers follow the same process as client desktop computers.

Domain controllers may nominate the primary domain controller (PDC) operations master as their in-bound time partner but may use a parent domain controller based on stratum numbering.

All PDC operations masters follow the hierarchy of domains in the selection of their in-bound time partner.

Following this hierarchy, the PDC operations master at the root of the forest becomes authoritative for the organization, and you should configure the PDC operations master to gather the time from an external source. This is logged in the System event log on the computer as event ID 62. Administrators can configure the Time service on the PDC operations master at the root of the forest to recognize an external Simple Network Time Protocol (SNTP) time server as authoritative by using the following »net time« command, where »server_list« is the server list:net time /setsntp:server_list

After you set the SNTP time server as authoritative, run the following command on a computer other than the domain controller to reset the local computer's time against the authoritative time server: net time /set

SNTP defaults to using User Datagram Protocol (UDP) port 123. If this port is not open to the Internet, you cannot synchronize your server to Internet SNTP servers.

NOTE: Administrators can also configure an internal time server as authoritative by using the »net time« command. If the administrator directs the command to the operations master, it may be necessary to reboot the server for the changes to take effect.

For additional information, see the following Microsoft white paper: The Windows Time Service

http://www.microsoft.com/windows2000/docs/wintimeserv.doc.«

Im Whitepaper »The Windows Time Service« finden Sie folgende Aussagen:

»The Net Time tool allows you to designate an external time source. It is important to note that even though the net time /? command returns a syntax that specifies that an »NTP List« can be designated, it is highly recommended that you only list one DNS name or IP address at a time. W32Time only recognizes the first DNS name or IP address listed and listing more than one might return an error.

To designate an external time source

At the command prompt, type:

net time /setsntp:DNSName – or – net time /setsntp:IPAddress

Many sites exist throughout the world that can be used for time synchronization. To find them, run a search for »time synchronization« on the Internet.

Currently, no time protocols in Windows 2000 work across forests and require that forests be in sync. However, PDC emulators in separate, independent forests need to be synchronized with the same globally correct time in order to provide for accurate time stamping on e-mail, log files, etc. ...

Is it necessary to synchronize time across forests?

Currently, no time protocols in Windows 2000 work across forests and require that forests be in sync. However, PDC emulators in separate, independent forests need to be synchronized with the same globally correct time in order to provide for accurate time stamping on e-mail, log files, etc.

Can a time server be run on any computer?

You can designate any computer as a time server by changing the value of the LocalNTP entry in the registry from 0 to 1. All registry entries for the Windows

Time Service are in the HKEY LOCAL MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters subkey. See Table 6 earlier in this article for a complete list of all registry entries associated with W32Time.

It is important to note that the automatic discovery mechanism in the time service client never chooses a computer that is not a domain controller. Clients must be manually configured to use any server that is not a domain controller.«

Sie müssen also am Domänencontroller der Stammdomäne den Befehl **net time /setsntp:*DNSName*** bzw. den Befehl **net time /setsntp:*IPAddress*** **absetzen.**

Das Freeware Tool **NetTime 2.0** hilft Ihnen, Zeitserver im Internet zu finden. Deren DNS-Name bzw. IP-Adresse können Sie dann im obigen Befehl einsetzen. Folgende Zeitserver können Sie z. B. im deutschsprachigen Raum nutzen:

```
ntp0.fau.de                 ntp1.fau.de
ntp2.fau.de                 ntps1-0.cs.tu-berlin.de
ntps1-1.cs.tu.berlin.de     ptbtime1.ptb.de
ptbtime2.ptb.de             rustime01.rus.uni-stuttgart.de
swisstime.ethz.ch           ntp0.nl.net
```

20.5 Datei- und Druckserver

Es ist weitgehend von der Anzahl der Benutzer eines Standortes und deren Arbeitsweise abhängig, wie groß das von den Benutzern erzeugte Dokumentvolumen ist, wie oft diese Dokumente angefasst und geändert werden, und mit welchem Zuwachs zu rechnen ist. Wenn der Großteil der Benutzer überwiegend mit kaufmännischen Anwendungen wie SAP arbeiten, aus diesen ERP-Anwendungen heraus Dokumente wie Geschäftsbriefe oder Rechnungen und Lieferscheine erzeugen und nur selten z. B. Microsoft Office Anwendungen wie Word, Excel, Access oder Powerpoint starten, wird ein performanter Datenbank-Server wichtiger sein als ein Datei- und Druckserver. Ist jedoch das Dokumentvolumen auf einem Dateiserver groß, geschäftskritisch und unterliegt es permanenten Zugriffen und einem großen Zuwachs, so kann es sinnvoll erscheinen, einen speziellen Mitgliedsserver als Datei- und Druckserver einzurichten, der also nicht durch zusätzliche Dienste wie Anmeldedienste, Active Directory-Replikation, RIS, DNS oder DHCP belastet wird.

Es kann sinnvoll sein, die Warteschlangen von Netzdruckern nicht auf den Dateiserver zu legen, sondern auf einen separaten Druckserver auszulagern und im Extremfall zur Steigerung der Ausfallsicherheit den Dateiserver zu clustern. Als Alternative zu einem Cluster kommt Distributed File System (DFS) infrage. Dabei werden bestimmte Verzeichnisse eines Servers wie z. B. das

22 Der Ausbau der Exchange Server-Organisation

In Kapitel 3, »Die Installation der Exchange-Organisation«, wurde ein Exchange Server nur rudimentär aufgesetzt, damit für die nachfolgenden Erläuterungen über Gruppenrichtlinien und die Office-Installation bereits ein Exchange Server verfügbar war. In diesem und den sich anschließenden Kapiteln erfolgt nun eine ganzheitliche Betrachtung des Produktes Exchange Server in einer Active Directory-Gesamtstruktur.

22.1 Kompatibilität zwischen Exchange 2000/2003 und Windows Server 2000/2003

Die Änderungen in Windows Server 2003 führten zur Registrierung von beinahe 350 Code-Änderungen, die sich auf Exchange 2000 Server auswirken. Diese Änderungen lassen sich in drei große Kategorien einteilen: Sicherheitsverbesserungen, Verbesserungen von IIS 6.0 und allgemeine Verbesserungen des Betriebssystems. In Windows Server 2003 wurden z. B. Änderungen für das Sperren von IIS vorgenommen, damit die Standardinstallation besser vor Angriffen geschützt ist. Ein Teil dieser Änderungen beziehen sich auf das standardmäßige Deaktivieren von ISAPI (Internet Server Application Programming Interface). Damit eine ausführbare Datei mit IIS-Anforderungen interagieren kann, muss sie mithilfe von ISAPI geschrieben werden. Das standardmäßige Deaktivieren von ISAPI bedeutet, dass bei einer Windows Server 2003-Standardinstallation IIS nur statische HTML-Dateien bereitzustellen kann. Um diese Sicherheitsänderung in Windows auszugleichen, wurde eine neue Architektur für das Exchange Server-Installationsprogramm erforderlich. Als Folge davon lässt sich unter Windows Server 2003 nur noch der Exchange Server 2003 installieren. Ältere Versionen des Exchange Servers können nicht unter Windows Server 2003 installiert werden.

Exchange Server 2003 unter Windows Server 2003 stellt eine Vielzahl neuer Funktionen zur Verfügung, beispielsweise die Unterstützung für Cluster mit acht Knoten, die Unterstützung für Volumenschattenkopie-Dienste und das neue »RPC über HTTP«-Protokoll, das Benutzern von Outlook 2003 die sichere und direkte Kommunikation mit dem Exchange Server 2003 über MAPI oder eine HTTP-Verbindung ermöglicht. Zwar kann Exchange Server 2003 auf einem Servercomputer installiert und ausgeführt werden, der Windows 2000 Server ausführt, diese neuen Funktionen erfordern jedoch, dass Exchange 2003 auf

einem Servercomputer mit einer Installation von Windows Server 2003 ausgeführt wird.

Dem Whitepaper »Microsoft Exchange Server – Kompatibilität mit Windows Server 2003« können Sie einige wichtige Aussagen bezüglich der Kompatibilität der Produkte Exchange 2000/2003 Server, Exchange 5.0/5.5 Server und Windows Server 2000/2003 entnehmen. Einige wichtige Aussagen werden nachfolgend zitiert:

> *»In der Produktfamilie des Windows-Betriebssystems sind viele Komponenten vorhanden, die inzwischen veraltet sind oder durch neuere Technologien ersetzt wurden. Um mögliche Sicherheitsrisiken zu vermeiden, die durch die veralteten Komponenten entstehen können, wurden einige dieser Komponenten aus der Standardinstallation oder aus dem gesamten Produkt entfernt.*
>
> *Durch Entfernen unnötiger Komponenten und Verzicht auf die Installation von Komponenten, die später durch unsachgemäße Verwaltung ein Sicherheitsrisiko darstellen können, beseitigt Windows Server 2003 die häufigsten Angriffspunkte, die Programmierer für unberechtigte Zugriffe verwenden.*
>
> *Microsoft Exchange 2000 Server und Microsoft Exchange 5.5 Server können nicht auf einem Servercomputer installiert und ausgeführt werden, der Windows Server 2003 ausführt. Exchange 2000 Server muss auf einem Computer mit Windows 2000 Server installiert werden. Exchange 5.5 kann auf einem Computer installiert werden, der Windows NT oder Windows 2000 Server ausführt.«*

Ein Exchange Server 2003 kann sowohl auf einem Windows Server 2003 als auch auf einem Windows 2000 Server installiert werden. Jedoch kann auf einem Windows Server 2003 weder ein Exchange Server 5.5 noch ein Exchange 2000 Server installiert werden. Exchange 5.5 Server kann auch in einer gemischten Windows 2000 Server- und Windows Server 2003-Umgebung vorhanden sein, obwohl der Exchange 5.5 Server das Active Directory nicht verwendet

22.2 Wichtige Exchange Server-Begriffe

Um das Zusammenspiel mehrerer Exchange Server in einer komplexeren Umgebung mit mehreren Standorten zu verstehen, müssen Sie einige Exchange-Begriffe beherrschen.

Exchange-Organisation

Organisation, administrative Gruppen und Exchange Server bilden die administrative Topologie der Exchange-Organisation. Der Organisationsname muss bei der Installation des ersten Exchange Servers bzw. bei der Ausführung von

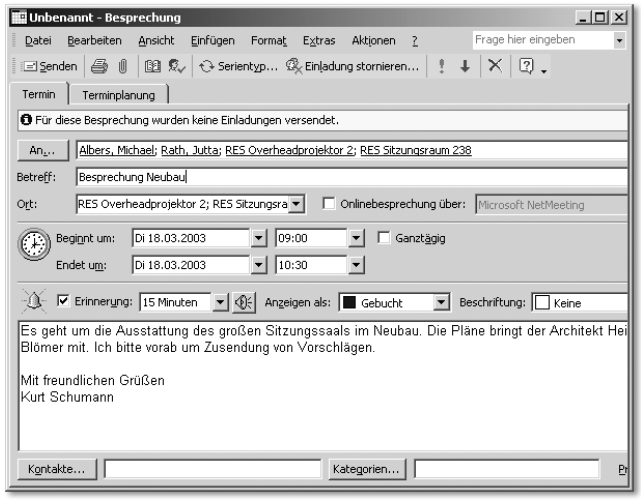
expliziten Verteilerlisten verzichten. Eine Ausnahme könnte z.B. sein, wenn Sie einen E-Mail-Verteiler benötigen, der sowohl Benutzerkonten der Domänen bzw. der Active Directory-Gesamtstruktur als auch externe Kontakte aufnehmen soll, weil es externe Projektmitarbeiter gibt.

Benutzer können sich über die Outlook-Kontakte selbst eigene Verteiler erstellen und in einen derartigen Verteiler auch externe Kontakte (z.B. einen externen Projektmitarbeiter) aufnehmen. Schulen Sie also für solche Zwecke ihre Mitarbeiter. Wenn für ein befristetes Projekt eine neue Verteilerliste angelegt werden soll, so machen Sie sich einen Erinnerungstermin in Ihren Terminkalender und fragen in regelmäßigen Abständen wieder nach, ob diese Projekt-Verteilerliste noch benötigt wird oder gelöscht werden kann. Halten Sie Ordnung in Ihren Verteilerlisten.

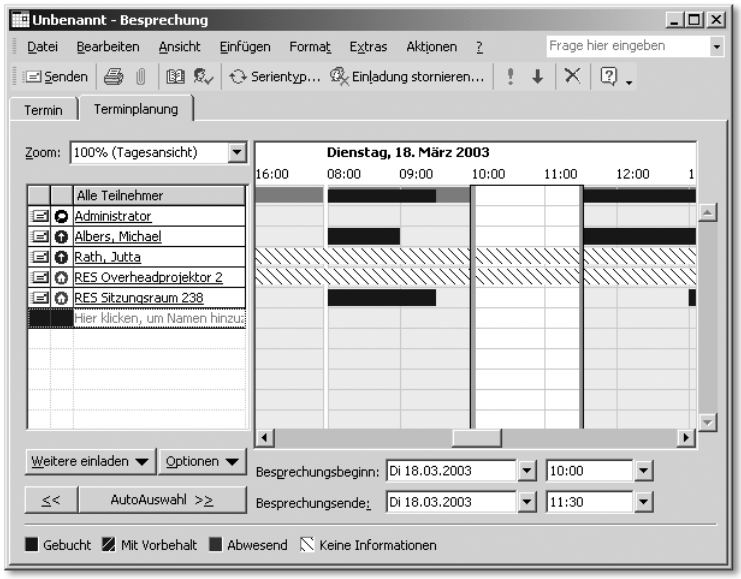
24.4 Ressourcen anlegen

Ressourcen sind z.B. Besprechungsräume, Dienstfahrzeuge, Beamer oder Overheadprojektoren. Eine Ressource wird, technisch gesehen, wie ein Mitarbeiterkonto angelegt, indem ein Postfach-aktiviertes Benutzerkonto für die Ressource erzeugt wird. Anschließend wird jedoch einem oder mehreren Mitarbeitern der Zugriff auf das Postfach dieser Ressource erlaubt, denn diese Mitarbeiter sollen die Ressource verwalten.

Wozu sind Ressourcen gut? Ein Beispiel: Ein Mitarbeiter möchte drei Kollegen zu einer Besprechung im Sitzungsraum 238 einladen. Er benötigt für eine Präsentation einen Overheadprojektor. Der Mitarbeiter startet Outlook und wählt **Datei · Neu · Besprechungsanfrage**. Er gibt das Thema der Besprechung an:



Jetzt möchte er herausfinden, ob und wann am Dienstag dem 18.03.2003 der gewünschte Besprechungsraum und ein Projektor verfügbar sind und die Kollegen Zeit haben. Dazu wählt er die Registerkarte **Teilnehmerverfügbarkeit**.



Über die Schaltfläche **Weitere einladen** können die gewünschten Kollegen und die benötigten Ressourcen ausgewählt werden. Wenn alle Mitarbeiter ihre Kalender unter Outlook pflegen und Ressourcen nicht mehr mündlich zugesagt werden, sondern nur noch über Outlook und Exchange Server, so kann der Mitarbeiter sehen, wann die Mitarbeiter und die gewünschten Ressourcen verfügbar sind. In obigem Beispiel würde der zuerst gewünschte Termin 8:00 Uhr sich mit einem anderen Termin überschneiden. Deshalb verschiebt der einladende Mitarbeiter die Balken auf die Zeitspanne 10:00 Uhr bis 11:30 Uhr, wechselt dann zurück zur Registerkarte **Termin** und wählt dann **Senden**.

Die Mitarbeiter, die die Ressourcen verwalten, erhalten eine Besprechungsanfrage für den Overheadprojektor und den Sitzungsraum 238. Wenn nichts dagegenspricht, wählen Sie die Schaltfläche **Zusagen**. Dadurch wird im Kalender der Ressource der Termin gebucht, und der einladende Mitarbeiter erhält eine Bestätigung, dass die Ressource den Termin akzeptiert oder der eingeladene Mitarbeiter zugesagt hat.

Im Unterkapitel 3.7 »Einfache Groupware- und Workflow-Funktionen nutzen« des Kapitels 3 »Die Installation der Exchange-Organisation« finden Sie weitere Anregungen, die Sie zusammen mit den Inhalten dieses Kapitels verwerten können, um eine Anleitung für Exchange-Administrationsaufgaben zu erstellen, mit der später die dezentralen Administratoren und Helpdesk-Mitarbeiter typische Administrationsaufgaben genormt durchführen können.

27 Einstieg in die Projektierung

Dieses Kapitel soll keine Projektplanung zur Einführung von Microsoft Active Directory ersetzen, sondern dem mit der Einführung des neuen Systems beauftragten Systemadministrator als Leitfaden für den Einstieg in die Projektierung dienen.

27.1 Ein möglicher Ablauf des Projekts zur Einführung von Active Directory

Nur wer bereits vom Start eines Projektes an »mit dem Schlimmsten rechnet« und ein aktives, vorausschauendes Risiko-Management betreibt, kann bereits in den »Genen« eines Projektes Vorkehrungen gegen Krisenfälle treffen. Die Projektsteuerung ist kein »Nebenjob«. Eine Vielzahl von Projekten scheitert nicht an zu hohen funktionalen Anforderungen oder Qualitätsmängeln der Software, sondern an den Folgen eines unzureichenden Projekt-Managements:

- unklare Zielvorgaben
- unrealistische Planungen
- mangelnde Verfügbarkeit von Ressourcen
- nicht funktionierende Eskalationsprozeduren

Ein Vollzeit-Projektleiter mit einschlägigen Erfahrungen und klaren Entscheidungskompetenzen ist bei komplexen Projekten wie der Einführung oder Migration nach Microsoft Active Directory unerlässlich. Sind Erfahrungen im Projektmanagement bei den eigenen Mitarbeitern noch nicht vorhanden, kann externe Hilfe nützlich sein.

Keep it simple and smart

IT-Projekte leiden häufig unter dem Problem zu großer Komplexität. Projektlaufzeiten, Projektkosten und das Risiko des Scheiterns steigen überproportional, wenn die Projektziele, der Funktionsumfang und der Integrationsgrad maximiert werden. Um dem zu begegnen, können Ziele in mittelfristige und langfristige Ziele aufgeteilt werden und das Gesamtprojekt in überschaubare Teilprojekte zerlegt werden, die dann nacheinander angegangen werden.

Projekt-Qualitätssicherung (PQS)

Die Projekt-Qualitätssicherung hat unter anderen folgenden Aufgaben:

- wirkungsvolles Risiko-Management
- neutrale Überwachung von fachlicher und technischer Ergebnisqualität
- Koordination eines Projekt-Lenkungsausschusses

Oft wird auf die explizite Besetzung dieser Rollen aus Gründen des Ressourcenmangels verzichtet. Um die Qualität des Projektergebnisses sicherzustellen und ein Scheitern des Projektes zu verhindern, sollten diese Funktionen jedoch nach Möglichkeit von Personen wahrgenommen werden, die nicht direkt in die Projektarbeit involviert sind.

In einer Art Projektskizze werden nachfolgend vieler Aufgaben und Probleme aufgelistet, die im Laufe des Projektes bewältigt werden müssen. Vorrangiges Ziel Ihrer eigenen Projektplanung muss sein, dass keine wesentlichen Dinge vergessen werden, die für die Planung der Ressourcen, des Zeitaufwands und des benötigten Budgets wichtig sind.

Auch die Art der Projektdokumentation müssen Sie selbst festlegen: Fließtext, Tabellen, Grafiken usw. Sie sollten schon zu Projektbeginn für die an der Erstellung aller Projektdokumentationen beteiligten Personen verbindlich festlegen, welche Tools und welche Anwendungsprogramme in welcher Version verwendet werden dürfen, damit jeder Projektmitarbeiter und auch jeder externe Mitarbeiter die einzelnen Teile der Projektdokumentation später einsehen und weiterbearbeiten können. Außerdem soll die Projektdokumentation später als Dokumentation des neuen Systems dienen und muss auch nach dem Projektende kontinuierlich weitergepflegt werden. Machen Sie also Vorgaben, mit welcher Textverarbeitung, Tabellenkalkulation und mit welchen Grafikprogrammen in welcher Version die Dokumentation erstellt werden soll. Diese Hilfsmittel sollten auch im Verlauf der weiteren Projektarbeit verwendet werden, damit die Dokumente nicht zueinander inkompatibel werden. Ebenso muss die gesamte Dokumentation ein eindeutiges Inhaltsverzeichnis und eine einheitliche Gestalt erhalten. Auch für ein Buchprojekt gibt ein Verlag eine Dokumentvorlage vor, damit das Buch später ein einheitliches Erscheinungsbild hat und der Leser sich leicht zurechtfindet.

Um das Projekt erfolgreich zu beenden, ist es außerdem wichtig, den Rahmen des Projekts abzugrenzen. Schon bei der Formulierung der Projektziele in Zusammenarbeit mit dem Auftraggeber ist es sinnvoll, schriftlich festzuhalten, was nicht zu den Projektzielen gehört. Diese Projektziele dürfen auch später nicht durch den Auftraggeber erweitert werden, zumindest nicht ohne eine Erweiterung der Ressourcen und des zeitlichen Projektrahmens. Es ist z. B. eindeutig zu klären, ob bzw. in welchem Rahmen die Einführung von Videokonferenzen, Multimedia, Telefonintegration, Telearbeit, Mobilcomputing usw. zum Projektumfang gehört.

Bereits in der ersten Projektphase sollten Sie eine möglichst detaillierte Ist-Aufnahme des Systems machen. Diese Ist-Aufnahme hat folgende Ziele:

- Sie können feststellen, wie detailliert Ihre IT-Infrastruktur dokumentiert ist und welchen Kenntnisstand Sie und das Projektteam über diese Infrastruktur haben.
- Sie können feststellen, welche Mitarbeiter des Unternehmens Wissensträger und Entscheidungsträger der IT-Infrastruktur sind.
- Sie können feststellen, welche Erwartungen andere Unternehmensbereiche an die Einführung von Active Directory haben und welche Ziele sie damit verknüpfen.
- Sie können feststellen, welche Sicherheitsprobleme es in der IT-Infrastruktur gibt und die Lösung dieser Probleme in den Anforderungskatalog aufnehmen.
- Sie können die Ist-Analyse als Grundlage für eine mittelfristige und eine langfristige Planung der anzustrebenden IT-Strukturen und der dafür notwendigen Budgetierung verwenden.
- Sie können den Kenntnisstand der eigenen Mitarbeiter in Bezug auf das vorhandene System und das einzuführende System eingrenzen und Rückschlüsse auf notwendige Schulungsmaßnahmen ziehen.

Wenn Sie ein externes IT-Systemhaus mit dem Projekt oder Teilen des Projektes beauftragen wollen, kann eine Ist-Aufnahme bereits bei den Vorgesprächen mit potenziellen IT-Systemhäusern wichtig sein.

- Sie können abstecken, welche Leistungen von eigenen Mitarbeitern erbracht werden können, und für welche Leistungen Sie externe Hilfe benötigen.
- Sie können bei der Einholung von Angeboten Teile oder eine Zusammenfassung der Ist-Analyse den infrage kommenden IT-Systemhäusern zur Verfügung stellen, die von externen Unternehmen zu erbringenden Leistungen katalogisieren und um die Abgabe eines detaillierten Konzeptvorschlages bitten. Aus den eingehenden Angeboten und Konzeptvorschlägen der IT-Systemhäuser können Sie bereits Rückschlüsse ziehen, welche Konzepte offensichtlich allgemein geltende Standards sind, und welche IT-Systemhäuser überhaupt in der Lage sind, konzeptionell und professionell zu arbeiten und das Projekt zu einem erfolgreichen Ende zu führen.
- Da externe Montagen teuer sind, können Sie viel Geld einsparen, wenn eine detaillierte Ist-Aufnahme und ein Soll-Konzept bereits vorliegen und nicht erst später von Mitarbeitern externer IT-Systemhäuser erstellt werden müssen.
- Eine detaillierte Ist-Aufnahme erleichtert die Einarbeitung weiterer interner und externer Projektmitarbeiter sowie Beratungsleistungen durch Lieferanten.

An die Ist-Analyse schließt sich die Erstellung des Soll-Konzeptes an. Sie erfolgt in der Regel nach der Top-Down-Methode, d. h. man geht vom Groben ins Detail. Ziele der Erstellung des Soll-Konzepts sind unter anderem Folgende:

- Es muss ein systematischer Aufgabenkatalog erstellt werden.
- Die logischen und zeitlichen Abhängigkeiten zwischen den einzelnen Aufgaben müssen transparent werden.

Am Ende dieses Vorgangs sollte ein Netzplan erstellt werden können, aus dem hervorgeht, in welcher Reihenfolge die Teilaufgaben abgearbeitet werden können, und welche Teilaufgaben parallel zueinander abgearbeitet werden können. Dieser Netzplan liefert den »kritischen Weg«. Das ist der zeitlängste Weg durch das Projekt, bei dem keine Zeitreserven mehr verfügbar sind. Verzögerungen auf dem kritischen Weg führen unweigerlich zur Verlängerung der Gesamtprojektdauer.

- Für die Teilaufgaben muss der personelle, zeitliche und monetäre Aufwand geschätzt werden. Die Summe dieser Aufwendungen für die Teilaufgaben ergibt den voraussichtlichen Gesamtaufwand des Projekts.
- Die Teilaufgaben müssen zu Arbeitspaketen zusammengestellt werden.
- Die Arbeitspakete müssen den internen und externen Projektmitarbeitern zugeordnet werden können.
- Der Schulungsbedarf für Projektmitarbeiter, Mitarbeiter der IT-Abteilung und für Endanwender muss ermittelt werden.
- Notwendige Anschaffungen müssen zusammengestellt werden. Diese umfassen Hardware- und Softwarebeschaffungen, Beschaffungen von Dienstleistungen (externe Beraterleistungen, externe Projektmitarbeiter, Schulungen für interne Projektmitarbeiter, Verträge mit Internet-Providern) sowie den Abschluss von Wartungsverträgen.
- Die Budgetierung für die Anschaffungen muss erfolgen.
- Ein Zeitplan für die Auslösung der Anschaffungsvorgänge muss erstellt werden.
- Es müssen so genannte »Projekt-Meilensteine« aufgestellt werden.

Bei Erreichen der Projekt-Meilensteine erfolgt eine Abnahme des Projektfortschritts durch den Projektauftraggeber. Ebenso erfolgt an den Projekt-Meilensteinen eine Kontrolle der bisherigen zeitlichen und monetären Aufwendungen und eine Risikoabschätzung für die verbleibenden Teilaufgaben. Dabei müssen unter anderem folgende Fragen geklärt werden:

- Kann das Projekt im zeitlich und finanziell geplanten Rahmen erfolgreich beendet werden?
- Reichen die personellen Ressourcen aus?
- Welche neuen Probleme sind aufgedeckt worden, und können sie gelöst werden?
- Gibt es Alternativen, wenn bestimmte Lösungswege nicht greifen?
- Bis zu welchen Zeitpunkten müssen welche Entscheidungen durchgefallen sein, die außerhalb der Entscheidungskompetenz der Projektleitung liegen?
- Sind notwendige Anschaffungsvorgänge zeitgerecht eingeleitet worden?
- Können die Lieferanten fristgerecht liefern?

Der nachfolgende Kriterienkatalog für eine Ist-Aufnahme und die Checkliste zur Erstellung eines Soll-Konzeptes erheben keinen Anspruch auf Vollständigkeit. Ebenso sind die Aufbaustruktur und der Grad an Detailliertheit nur beispielhaft. Da ein Soll-Konzept zur Einführung von Microsoft Active Directory, Exchange Server und Microsoft Office von Unternehmen zu Unternehmen sehr unterschiedlich ausfallen wird, kann die Checkliste zur Erstellung des Soll-Konzeptes exemplarisch einen Eindruck vermitteln, wie das Projektteam die Problemkreise sammelt, systematisiert und immer tiefer in Detailfragen zerlegt. Erst, wenn alle offenen Fragen ausformuliert wurden und strukturiert in einer logischen Reihenfolge vorliegen, sind der Projektumfang und zumindest ansatzweise auch der Projektablauf sowohl für den Auftraggeber als auch für die Projektmitarbeiter ausreichend vorgegeben.

27.2 Ist-Analyse

27.2.1 Analyse der Aufbau- und Ablauforganisation

- Skizzieren Sie z.B. in Form eines Organigramms den aktuellen Aufbau Ihrer Organisation.
- Erstellen Sie eine Abbildung aller Standorte mit den verfügbaren WAN-Leitungen zwischen den Standorten sowie deren Bandbreite.
- Benennen und beschreiben Sie den Zweck aller Standorte, Bereiche, Abteilungen und Abteilungsgruppen.
- Listen Sie die Anzahl der Netzwerkbenutzer in jedem Bereich der Organisation, die Anzahl der Netzwerkbenutzer an jedem Standort sowie die Gesamtanzahl der Netzwerkbenutzer auf.
- Beschreiben Sie, wie die Netzwerkbenutzer der einzelnen Abteilungen momentan das Netzwerk nutzen (Betriebssysteme, Anwendungen, Dienste).

Wartung/Fernwartung

Eine Wartung durch externe Stellen darf nur aufgrund schriftlicher Vereinbarungen erfolgen. Darin sind die im Rahmen der Wartung notwendigen technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit festzulegen. Die mit den Wartungsarbeiten betrauten Personen sind zur Wahrung des Datengeheimnisses zu verpflichten.

28.10 Der innerbetriebliche Datenschutzbeauftragte

Nach § 36 BDSG muss der Arbeitgeber in Betrieben, in denen personenbezogene Daten automatisiert verarbeitet werden, und die regelmäßig mindestens fünf Arbeitnehmer beschäftigen, einen Datenschutzbeauftragten benennen. Zum Beauftragten für den Datenschutz darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Der Beauftragte ist bei Anwendung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei und darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. Der Datenschutzbeauftragte ist für die Überwachung und Kontrolle der Datenverarbeitung hinsichtlich der gültigen Datenschutzgesetze verantwortlich. Schwerpunkte seiner Tätigkeit sind:

- Prüfung der Zulässigkeit des Umgangs mit Daten,
- Überwachung der ordnungsgemäßen Programmanwendung,
- Unterrichtung von Mitarbeitern über die Anforderungen des Datenschutzes.

Der Arbeitgeber muss dem Datenschutzbeauftragten nach § 36, Absatz 5 die zur Erfüllung der Kontrollaufgabe nötigen Hilfsmittel, nötiges Personal und nach § 37 als wichtiges Arbeitsmittel u. a. eine Dateienübersicht und eine Übersicht der eingesetzten DV-Anlagen zur Verfügung stellen.

Für die Kontrolle des Datenschutzes bei den nicht-öffentlichen Stellen sind die Aufsichtsbehörden der Länder zuständig. Die Aufsichtsbehörde überprüft ebenfalls die Ausführung des BDSG und anderer Vorschriften zum Datenschutz; im Allgemeinen allerdings nur, wenn Anhaltspunkte für einen Datenschutzverstoß vorliegen.

28.11 Musterformular für eine von allen Mitarbeitern zu unterschreibende Datenschutzverpflichtung

Nachfolgend finden Sie ein Musterformblatt für eine Verpflichtungserklärung auf den Datenschutz. Dieses Muster kann Ihnen als Anregung für die Erstellung eines eigenen Formulars dienen, das Sie von allen Mitarbeitern unterschreiben lassen sollten. Erkundigen Sie sich beim Datenschutzbeauftragten Ihres Bun-

deslandes nach zusätzlichen Rechtsvorschriften, die in Ihrem Bundesland gelten.

Dieses Formblatt beinhaltet nur Minimalansprüche für die Sicherheit der persönlichen Daten. Darüber hinaus sollten die Mitarbeiter natürlich auch zur Verschwiegenheit über Firmendaten verpflichtet werden: Daten über Produktionstechnologien und Forschungsergebnisse, über Organisations- und Marketing-Know-how, über Kunden- und Lieferantendaten usw. So können Sie die Mitarbeiter unterschreiben lassen, dass

- Daten weder auf Datenträgern wie Disketten oder Festplatten oder in gedruckter Form das Betriebsgelände verlassen dürfen,
- Daten nur mit Zustimmung des Vorgesetzten, Abteilungsleiters oder Datenschutzbeauftragten das Betriebsgelände verlassen dürfen,
- keine Daten über elektronische Kommunikationskanäle (Fax, E-Mail, Internet- oder CompuServe-Zugang) verschickt werden dürfen,
- keine fremde Software auf lokale Festplatten oder den Server ohne Zustimmung des Abteilungsleiters oder des Systemadministrators eingespielt werden dürfen,
- nicht versucht werden darf, auf Bereiche des LANs oder WANs vorzudringen, die nicht für den Anwender und sein Aufgabengebiet freigegeben sind, usw.

Ferner sind die Konsequenzen darzulegen, wenn ein Mitarbeiten gegen diese Regeln verstößt.

Verpflichtung nach § 5 Bundesdatenschutzgesetz – BDSG

§ 2 Abs. 2 Datenschutzgesetz Nordrhein-Westfalen – DSG NW

Herr / Frau _____(Name) _____(Vorname) ist nach § 5 BDSG / § 2 Abs. 2 DSG NW auf das Datengeheimnis verpflichtet und auf die Strafbarkeit einer Geheimnisverletzung nach § 43 BDSG ausdrücklich hingewiesen worden.

Nach § 5 BDSG ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten oder zu nutzen. Die Verpflichtung bezieht sich auf alle zu einer natürlichen Person gehörenden Angaben über deren persönliche und sachliche Verhältnisse. Die Verpflichtung auf das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.

Nach § 43 BDSG wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wer unbefugt von diesem Gesetz geschützte personenbezogene Daten, die nicht offenkundig sind

- speichert, verändert oder übermittelt,
- zum Abruf mittels automatisierten Verfahrens bereithält oder
- abruft oder sich oder einem anderen aus Dateien verschafft.

Ebenso wird bestraft, wer

- die Übermittlung von durch dieses Gesetz geschützten personenbezogenen Daten, die nicht offenkundig sind, durch unrichtige Angaben erschleicht,
- entgegen § 16 Abs. 4 Satz 1, § 28 Abs. 4 Satz 1, auch in Verbindung mit § 29 Abs. 3, § 39 Abs. 1 Satz 1 oder § 40 Abs. 1 die übermittelten Daten für andere Zwecke nutzt, indem er sie an Dritte weitergibt, oder
- entgegen § 30 Abs. 1 Satz 2 die in § 30 Abs. 1 Satz 1 bezeichneten Merkmale oder entgegen § 40 Abs. 3 Satz 3 die in § 40 Abs. 3 Satz 2 bezeichneten Merkmale mit den Einzelangaben zusammenführt.

Handelt der Täter gegen Entgelt oder in der Absicht, einen anderen zu schädigen oder sich oder einen anderen zu bereichern, so ist die Strafe eine Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

Zum Schutz personenbezogener Daten ist im Rahmen der zugewiesenen Aufgabe die notwendige Sorgfalt anzuwenden. Bestehende Vorschriften über den Umgang bzw. die Sicherung personenbezogener Daten sind zu beachten. Festgestellte Mängel sind möglichst umgehend zu melden.

Sonstige Geheimhaltungspflichten bleiben durch diese Verpflichtung unberührt.

Musterstadt, (Ort / Datum) (Unterschrift des Verpflichteten)

28.12 Mustervereinbarung zur Regelung datenschutzrelevanter Sachverhalte bei Reparaturen, technischen Wartungsarbeiten und Austausch von Komponenten an PC und Servern ohne Software-Pflege

§ 1
Geheimhaltung von Daten

1. Der Auftragnehmer verpflichtet sich, bei technischen Reparaturen, technischen Wartungsarbeiten oder Austausch von Komponenten auf gespeicherte Daten nur insoweit zuzugreifen, wie es die nachfolgenden Bestimmungen gestatten.

2. Sollten dem Auftragnehmer Inhalte von Datenbeständen bekannt werden, verpflichtet er sich, diese geheim zu halten.

3. Der Auftragnehmer verpflichtet sich, das bei Reparaturen, technischen Wartungsarbeiten oder beim Austausch von Komponenten eingesetzte Personal in der gleichen Weise zu verpflichten, und die so begründeten Geheimhaltungspflichten zu überwachen.

4. Die Vergabe von Unteraufträgen ist nur mit Zustimmung des Auftraggebers zulässig. Bei Unteraufträgen, die der Auftraggeber genehmigt hat, hat der Auftragnehmer den Unterauftragnehmer in gleicher Weise zu verpflichten. Für den Unterauftragnehmer gilt § 1 Absatz 1 entsprechend.

5. Der Auftragnehmer sichert dem Auftraggeber zu, dass er nach Abschluss der Arbeiten alle Daten des Auftraggebers, die er während der Arbeiten kopiert oder ausgedruckt hat, unverzüglich löschen oder vernichten wird. Datenträger, die der Auftraggeber für die Arbeiten zur Verfügung gestellt hat, sind dem Auftraggeber unmittelbar nach Abschluss der Arbeiten wieder auszuhändigen.

§ 2
Sparsame Datenverwendung

1. Ist der Zugriff auf Daten wegen der Art der vereinbarten Reparaturen, der technischen Wartungsarbeiten oder wegen des Austauschs von Komponenten unvermeidbar, so verpflichtet sich der Auftragnehmer, den Datenzugriff auf das unverzichtbare Mindestmaß zu beschränken.

2. Setzen die Arbeiten einen Zugriff auf personenbezogene Daten zwingend voraus, informiert der Auftragnehmer den Auftraggeber. Der Auftraggeber entscheidet, wie in derartigen Fällen vorzugehen ist.

3. Gestattet der Auftraggeber den Zugriff auf ausgewählte personenbezogene Datenbestände, so dürfen die vereinbarten Arbeiten ausschließlich mit diesen Datenbeständen ausgeführt werden.

4. So weit wegen der Art der vereinbarten Reparaturen, technischen Wartungsarbeiten oder beim Austausch von Komponenten ein Zugriff auf personenbezogene Daten erfolgt, dürfen keine Veränderungen vorgenommen werden. Versehentlich vorgenommene Veränderungen sind dem Auftraggeber bekannt zu geben.

5. Änderungen an Systemdateien, die im Zuge der Arbeiten erforderlich geworden sind, müssen vom Auftragnehmer dokumentiert werden. Auf Verlangen des Auftraggebers sind solche Veränderungen nach Abschluss der Arbeiten rückgängig zu machen.

§ 3
Austausch von Komponenten

1. Beim Austausch von Komponenten, mit denen Daten dauerhaft gespeichert werden können, insbesondere Festplattenlaufwerke und ähnliche Speichermedien, stellt der Auftragnehmer sicher, dass entnommene Komponenten nach Abschluss der Arbeiten in einer Weise zerstört werden, die den Zugriff oder eine Wiederherstellung von Daten technisch ausschließt.

2. Wünscht der Auftraggeber die Aushändigung von ausgetauschten Komponenten, so sind diese bis zur Übergabe unter Verschluss zu halten.

§ 4
Übertragung von Speicherinhalten

1. Umfasst der Auftrag das Kopieren gespeicherter Daten, die sich auf ersetzten Komponenten oder beschädigten Speichermedien befunden haben, so ist ein Kopierverfahren zu verwenden, das die Anzeige des Inhalts von Datenbeständen so weit wie möglich vermeidet. § 1 Abs. 2 und § 2 Abs. gelten entsprechend.

2. Nach der Übertragung sind die entnommenen Komponenten oder die überlassenen Speichermedien vollständig zu löschen oder zu vernichten. Wenn der Auftraggeber das wünscht, sind sie ihm unverändert und ungelöscht auszuhändigen.

§ 5
Schadensersatz

1. Wird der Inhalt von Datenbeständen entgegen der Geheimhaltungspflichten Dritten bekannt, hat der Auftragnehmer den dadurch entstehenden Schaden zu ersetzen. Zum ersatzpflichtigen Schaden gehören auch Zahlungen, die der Auftraggeber Dritten zu leisten hat.

2. Den Nachweis für fehlendes Verschulden hat der Auftragnehmer zu erbringen.

3. Für ein Verschulden ihres Personals haften Auftragnehmer und Unterauftragnehmer in gleicher Weise wie für eigenes Verschulden.

Unterschrift Auftraggeber Unterschrift Wartungsfirma