UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

backUP

MAGAZIN FÜR IT-SICHERHEIT

backUp Magazin für IT-Sicherheit

05 / 2003

Ausgabe
Nr. 05
2003

MS-WINDOWS 2000

Sicherheitsmaßnahmen und Restrisiken

HERAUSGEBER: Unabhängiges Landeszentrum
für Datenschutz Schleswig-Holstein
Postfach 71 21 | 24171 Kiel
Ansprechpartner: Heiko Behrendt
Telefon: (0431) 988 - 12 12 | Telefax: (0431) 988 - 12 23
E-Mail: mail@datenschutzzentrum.de
Homepage: www.datenschutzzentrum.de

TITEL-DESIGN: Eyekey Design, Kiel
www.eyekey.de

DRUCK: Druckerei A.C. Ehlers, Kiel

AUFLAGE: 1. Auflage, Juni 2003

Vorwort

Liebe Leserinnen, liebe Leser!

Wer einen Tresor in eine dünne Pappwand einbaut, wird nicht viel Sicherheit gewinnen. Ähnlich verhält es sich, wenn an Datensicherheit erst bei der Anwendungssoftware gedacht wird und nicht bereits auf der Betriebssystemebene.

Bei der Entwicklung und Verbreitung der PC standen zunächst Rechnerleistung und niedriger Preis im Vordergrund, Sicherheit spielte eine untergeordnete Rolle. Ein verhängnisvoller Fehler, weil die PC keineswegs nur im häuslichen Wohnzimmer für Computerspiele genutzt werden, sondern überall in Wirtschaft und Verwaltung zum Einsatz kommen.

Microsoft reagierte auf die Kritik an den Sicherheitsdefiziten seiner Standardprodukte und führte erstmals mit Windows NT 4.0 spezifische Sicherheitsmechanismen ein. Windows 2000 setzt diese Linie fort. Allerdings sind zur Implementation der Sicherheitsfunktionen zumeist Kenntnisse über das übliche Heimwerkerniveau hinaus notwendig.

Mit der Reihe unserer ***backUP***-Magazine (zu dieser Thematik sind bisher erschienen: „MS-Windows NT 4.0 – Sicherheitsmaßnahmen und Restrisiko“ sowie „MS-Windows NT 4.0 – Resource Kit und Security-Tools“) wollen wir Administratoren und privaten Nutzern von Microsoft-Produkten Unterstützung bei der Verbesserung der Datensicherheit geben. Das jetzt vorliegende ***backUP***-Magazin „MS-Windows 2000 – Sicherheitsmaßnahmen und Restrisiko“ ist doppelt so umfangreich wie die ***backUP***-Magazine zu Windows NT 4.0. Das zeigt, dass den Administratoren und anderen Interessenten wesentlich mehr Know-how vermittelt werden muss, um die komplexen Sicherheitsfunktionen richtig einsetzen zu können.

Die ***backUP***-Magazine sind eine Serviceleistung des Unabhängigen Landeszentrums für Datenschutz. Sie werden ergänzt und abgerundet durch die Spezialkurse der DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN. Ich würde mich über Kritik und Anregungen zur Optimierung unserer ***backUP***-Magazine freuen und wünsche viel Spaß bei der Verbesserung der Sicherheit Ihres Betriebssystems.

Kiel, im Juni 2003

Dr. Helmut Bäumler

Landesbeauftragter für den Datenschutz

Inhalt

1 Grundlagen

In diesem Kapitel erfahren Sie,

- wie das ***backUP-Magazin*** zu benutzen ist,
- welche Rechtsvorschriften bei der Erarbeitung von Sicherheitskonzepten zu beachten sind und
- welche Rahmenbedingungen für die Umsetzung von **technischen** Sicherheitsmaßnahmen geschaffen werden müssen.

1.1 Einleitung

Die Reihe ***backUP***-Magazine[1] wird mit dem ***backUP***-Magazin **„Windows 2000 – Sicherheitsmaßnahmen und Restrisiken“** erweitert. Dieses Heft soll die IT-Betreuer unterstützen, technische Sicherheitsmaßnahmen unter dem Betriebssystem MS Windows 2000 auf der Arbeitsplatz- und Serverebene zu implementieren. Schwachstellen werden erläutert und Lösungen für ihre Beseitigung aufgezeigt. Darüber hinaus werden nicht nur technische Aspekte behandelt, sondern ebenso Grundlagen in Bezug auf die Sicherheitsproblematik beim Einsatz von MS Windows 2000-Systemen vermittelt. Deshalb sollte sich auch die Leitungsebene sowie der/die Datenschutzbeauftragte mit der Thematik vertraut machen. Weiterhin kann dieses Magazin dazu benutzt werden, bereits unter MS Windows 2000 realisierte Sicherheitseinstellungen auf ihre Wirksamkeit hin zu überprüfen.

Es zeichnete sich bereits während der Erstellung ab, dass aufgrund der Komplexität des neuen Betriebssystems nicht alle Sicherheitsaspekte umfassend beschrieben werden konnten. Der Umfang hätte den Rahmen gesprengt, und die Übersicht für den Leser wäre verloren gegangen. Nicht angesprochene und nur kurz erläuterte Sicherheitsaspekte werden deshalb voraussichtlich in einem hierauf aufbauenden ***backUP-***Magazin aufgegriffen.

Wie in allen anderen ***backUP-***Magazinen liegt der Schwerpunkt der Darstellung auf einer guten Verständlichkeit und der Möglichkeit der praktischen Umsetzung. An dieser Stelle sei

---

[1] *backUP* Nr. 1: IT-Sicherheitskonzepte: Planung – Erstellung – Umsetzung
backUP Nr. 2: MS-Windows NT 4.0 – Sicherheitsmaßnahmen und Restrisiken
backUP Nr. 3: MS-Windows NT 4.0 – Resource Kit und Security -Tools
backUP Nr. 4: PC-Arbeitsplatz – So viel Datenschutz muss an jedem Arbeitsplatz sein!

erwähnt, dass die ***backUP***-Magazine auch als Grundlage für die technikorientierten Kurse der DATENSCHUTZAKADEMIE[2] Schleswig-Holstein dienen.

1.2 Hinweise für die Benutzung

Dieses ***backUP***-Magazin erhebt keinen Anspruch auf die umfassende Vermittlung der Windows 2000-Theorie, vielmehr soll es als ein praktischer Ratgeber den IT-Betreuern die Arbeit unter datenschutzrelevanten Gesichtspunkten erleichtern. Für eine planvolle und sichere Administration sollten die im Anhang aufgelisteten Fachbücher oder die Windows 2000-Hilfe mit herangezogen werden, da die Administrationsschritte hier nur kontextbezogen beschrieben werden können.

Es werden folgende Schreibweisen verwendet, um Schaltflächen, Befehle und Definitionen unterscheiden zu können:

- **Schaltflächen**, Verzeichnisnamen, Registerkarten usw. werden, wie bei HINZUFÜGEN, in Kapitälchen gesetzt.
- **Befehle**, wie `net use`, werden in nicht proportionaler Schrift gesetzt.
- **Eigennamen**, wie *Hardwarekompatibilitätsliste,* werden kursiv dargestellt.
- **Internetadressen**, wie <www.microsoft.com/hwtest/hcl>, und Verzeichnispfade, wie <E:\I386\Winnt32>, werden in eckige Klammern gesetzt.

Zur Verbesserung der Orientierung ist der Text in bestimmte Funktionsabschnitte gegliedert, die durch entsprechende Symbole gekennzeichnet sind. Folgende Symbole finden Verwendung:

Weist auf Inhalte hin, die bei der Planung von Aufgaben nützlich sein können. Eine so gekennzeichnete Vorgehensweise sollte mit der Leitungsebene abgestimmt werden.

[2] Das Kursangebot ist im Jahresprogramm der DATENSCHUTZAKADEMIE Schleswig-Holstein abgedruckt und beim ULD erhältlich, Näheres unter <www.datenschutzzentrum.de/akademie/>.

*Kennzeichnet **Hinweise**, die für die Umsetzung von Sicherheitsmaßnahmen von **entscheidender** Bedeutung sind. Die beschriebenen Empfehlungen sollten in jedem Fall beachtet werden.*

Beschreibt im Detail die Arbeitsschritte, die für die Umsetzung einer Sicherheitsmaßnahme oder für die Einstellung einer technischen Funktion notwendig sind.

Achtung! Hier ist bei administrativen Maßnahmen Vorsicht geboten!

Die beschriebenen Sachverhalte sollten unbedingt überprüft und die dargestellten Sicherungsvorkehrungen oder Administrationshilfen beachtet werden.

Beschreibt zusammenfassend die Sicherheitsmaßnahmen und die Informationen, die beim Einsatz von Windows 2000 berücksichtigt werden sollten.

1.3 Rechtsgrundlagen der Datenverarbeitung

Für die Verarbeitung personenbezogener Daten gelten je nach Organisationsform (öffentliche oder nichtöffentliche Stelle) die bereichsspezifischen landes- und bundesrechtlichen Vorschriften, die einschlägigen Vorschriften des Landesverwaltungsgesetzes und ggf. vertraglich vereinbarte Regelungen. Ergänzend sind die Bestimmungen des Landesdatenschutzgesetzes (LDSG) und der Datenschutzverordnung (DSVO) bzw. des Bundesdatenschutzgesetzes (BDSG) zu beachten.

§ 5 Abs. 2 S. 1 LDSG 2000 (öffentliche Stellen des Landes Schleswig-Holstein):

„Es sind die technischen und organisatorischen Maßnahmen zu treffen, die nach dem Stand der Technik und der Schutzbedürftigkeit der Daten erforderlich und angemessen sind."

§ 9 DSVO (öffentliche Stellen des Landes Schleswig-Holstein):

„Durch technische und organisatorische Maßnahmen ist sicherzustellen, dass verändernde Zugriffe auf Programme zur Systemsteuerung und auf freigegebene Anwendungsprogramme und Verfahren nur durch dazu ausdrücklich befugte Personen erfolgen können und diese durch weisungsbefugte Mitarbeiterinnen oder Mitarbeiter oder deren Beauftragte kontrolliert werden."

§ 9 BDSG (öffentliche Stellen des Bundes, nichtöffentliche Stellen):

„Öffentliche und nichtöffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht."

1.4 IT-Sicherheitskonzept

Die IT-Sicherheit ist für jedes IT-Projekt, jedes IT-System und alle IT-Nutzer innerhalb einer Organisation zu gewährleisten. Als Grundlage für die Umsetzung von konkreten IT-Sicherheitsmaßnahmen dient deshalb das **IT-Sicherheitskonzept**. In ihm werden alle technischen und organisatorischen Sicherheitsmaßnahmen dargestellt, die erforderlich und angemessen sind, um den von den IT-gestützten Verarbeitungsprozessen ausgehenden Gefahren zu begegnen. Öffentliche Stellen können ihr Datenschutzkonzept durch das Unabhängige Landeszentrum für Datenschutz im Rahmen eines **Datenschutzaudits** prüfen und beurteilen lassen.[3]

[3] Alle öffentlichen Stellen in Schleswig-Holstein können entweder für ihre gesamte Datenverarbeitung, für abtrennbare Teile hiervon oder für einzelne Datenverarbeitungsverfahren ein Datenschutzaudit beantragen.

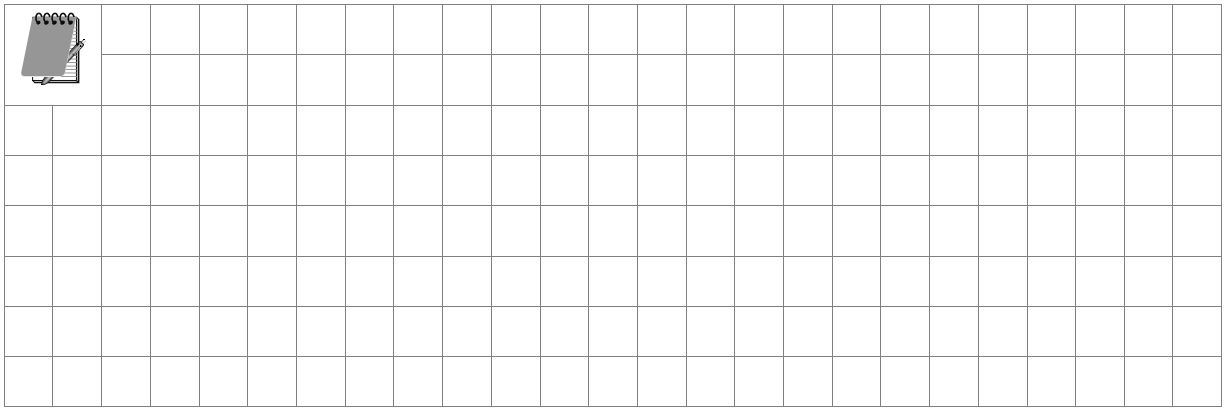
1.5 Rahmenbedingungen

Die Gestaltung einer Client/Server-Architektur unter Windows 2000 erfordert eine intensive Planung und ihre ständige Anpassung an Veränderungen der Aufbau- und Ablauforganisation der Daten verarbeitenden Stelle. Ebenso ist **ausreichend** administratives Personal sowie eine gründliche **Schulung** der Administratoren erforderlich.

Besonders wichtig ist eine zielgerichtete und konsequente Vorgehensweise bei der Umsetzung technischer Sicherheitsmaßnahmen. Das setzt zunächst voraus, dass die von der **Leitungsebene** festgelegten Vorgaben und die unter Windows 2000 verfügbaren Sicherheitsfunktionen bekannt sind. Es ist darüber hinaus dringend zu empfehlen, im Rahmen eines Pilotprojektes die Sicherheitsmaßnahmen zunächst in einer **Testumgebung** zu erproben.

1.6 Sicherheitscheck

- *In Bezug auf die Auswahl der **Sicherheitsmaßnahmen** sind die bereichsspezifischen landes- und bundesrechtlichen Vorschriften sowie die Bestimmungen des LDSG und der DSVO bzw. des BDSG zu beachten.*
- *Als **Grundlage** für die Umsetzung der Sicherheitsmaßnahmen dient ein Sicherheitskonzept.*
- *Die technische Umsetzung des Sicherheitskonzeptes setzt eine **geplante** Vorgehensweise voraus.*
- *Der IT-Bereich muss **personell ausreichend besetzt** und fachlich geschult sein.*
- *Die **IT-Betreuer** sollten auch in kritischen Situationen in der Lage sein, die technischen Sicherheitskomponenten der Server und der Arbeitsstationen ordnungsgemäß zu administrieren.*



2 Überblick Windows 2000

In diesem Kapitel erfahren Sie,

- welche Windows 2000-Versionen verfügbar sind,
- welche Systemanforderungen an die Hardware gestellt werden,
- wofür die Managementkonsole eingesetzt wird,
- was das Active Directory darstellt und welche Bedeutung es hat,
- welche neuen Funktionen Windows 2000 gegenüber Windows NT enthält und
- welche Tools sich auf dem Windows 2000-CD-Satz befinden.

2.1 Windows 2000

Mit Windows 2000 hat Microsoft nach eigenen Aussagen in der Entwicklung der Betriebssystem-Produktlinie einen bedeutenden Schritt nach vorne gemacht. Große Aufmerksamkeit sei insbesondere der Sicherheit gewidmet worden. *Active Directory* stelle das Kernstück von Windows 2000 dar.

Windows 2000 wird in vier Versionen ausgeliefert:

- **Windows 2000 Professionell** als Betriebssystem für den Arbeitsplatzrechner,
- **Windows 2000 Server** für kleine bis mittlere Organisationen,
- **Windows 2000 Advanced Server** für mittlere bis große Organisationen,
- **Windows 2000 Datacenter Server** für sehr große Organisationen.

Die verschiedenen Server-Versionen unterscheiden sich hauptsächlich in den Leistungsmerkmalen für die Unterstützung von Multiprocessing, Festplattenverwaltung (Clustering) sowie den Lastenausgleich beim Einsatz mehrerer Windows 2000 Server. Im Bereich der Verwaltung und in den mittleren Wirtschaftsunternehmen wird in der Regel der Einsatz von Windows 2000 Server ausreichend sein.

Viele Server, auf denen Windows NT 4.0 installiert ist, verfügen nicht über die Hardwarekomponenten, die zum Ausführen von Windows 2000 erforderlich sind. Zur Aktualisierung dieser Server und Beibehaltung der Systemkonfiguration müssen Sie zunächst die Systemhardware unter Windows NT 4.0 aktualisieren (siehe Kapitel 3).

In der folgenden Tabelle sind die Systemanforderungen an die Hardware für die Installation von Windows 2000 aufgelistet:

Komponente	**Windows 2000 Professional**	**Windows 2000 Server**
CPU	mindestens Pentium 133 MHz Windows 2000 Professional unterstützt bis zu 2 Prozessoren Windows 2000 Server unterstützt bis zu 4 Prozessoren Windows 2000 Advanced Server unterstützt bis zu 8 Prozessoren Windows 2000 Datacenter Server unterstützt bis zu 16 Prozessoren	
Arbeitsspeicher	mindestens 64 MB maximal 4 GB	mindestens 256 MB maximal 4 GB (2000 Server) maximal 8 GB (2000 Advanced Server)
Speicherplatz	2 GB mit mindestens 1 GB freiem Arbeitsspeicher	
Anzeige	VGA-Monitor mit höherer Auflösung	
Laufwerke	CD-ROM, 12x oder schneller	
Netzwerk	Windows 2000-kompatible Netzwerkkarte	

Vor der Installation ist zu prüfen, ob die Hardware in der *Hardwarekompatibilitätsliste* (HCL) aufgeführt ist. Microsoft stellt nur für solche Geräte getestete Treiber bereit, die in der Windows 2000-HCL aufgelistet sind. Das Verwenden von Hardware, die nicht in der HCL aufgeführt ist, verursacht möglicherweise Probleme während und nach der Installation. Eine Kopie der HCL befindet sich in der Datei hcl.txt im Ordner SUPPORT auf der Windows 2000-CD.

Von der Microsoft-Website <www.microsoft.com/hwtest/hcl> kann die aktuelle Version der HCL heruntergeladen werden.

2.1.1 Windows 2000 Server

Der Windows 2000 Server ist mithilfe des Assistenten bzw. des Verwaltungsprogramms *Konfiguration des Servers* zu konfigurieren. Vor der Einrichtung des Servers ist festzulegen, ob er als Domänencontroller, als Mitgliedsserver oder als allein stehender Server konfiguriert werden soll.

Domänencontroller

Bei einem Domänencontroller handelt es sich um einen Computer, auf dem Windows 2000 Server ausgeführt wird und *Active Directory* eingerichtet wurde. Mit dem *Assistent zur Installation von Active Directory* werden Komponenten installiert und konfiguriert, die Netzwerkbenutzern und Computern den Active Directory-Verzeichnisdienst zur Verfügung stellen. Domänencontroller dienen zur zentralen Verwaltung von Objekten und managen die Benutzeranmeldung und -authentifizierung sowie den Zugriff auf Verzeichnisse und Ressourcen in einem Netzwerk.

Mitgliedsserver

Ein Mitgliedsserver ist ein Computer, der Windows 2000 Server-Dienste ausführt, aber kein Domänencontroller einer Windows 2000-Domäne ist. Mitgliedsserver sind Mitglieder in einer Domäne, auf denen keine Kopie der Active Directory-Datenbank gespeichert wird. Es können Berechtigungen für die Ressourcen des Mitgliedsservers festgelegt werden, mit denen Benutzer eine Verbindung mit dem Server herstellen und dessen Ressourcen verwenden können.

Allein stehender Server

Ein allein stehender Server ist ein Computer, der Windows 2000 Server-Dienste ausführt, aber kein Domänencontroller oder Mitglied einer Windows 2000-Domäne ist. Ein allein stehender Computer speichert nur seine eigene Benutzerdatenbank und verarbeitet Anmeldeanforderungen selbstständig. Kontoinformationen werden nicht für andere Computer freigegeben, und der Zugriff auf Domänenkonten ist nicht möglich.

Über den Assistenten kann der Windows 2000 Server wie folgt konfiguriert werden:

- **Active Directory:** Der Server wird mit der Installation von Active Directory zum Domänencontroller hochgestuft. Es ist ebenfalls möglich, einen Domänencontroller wieder herabzustufen. Dieser Schritt muss jedoch sorgfältig überdacht sein, da in diesem Fall alle im Active Directory enthaltenen Informationen dieses Domänencontrollers verloren gehen.

- **Dateiserver:** Über die Funktion Dateiserver können Freigabeberechtigungen auf Ordner des Servers vergeben werden.
- **Druckserver:** Mit der Funktion Druckserver können auf dem Windows 2000 Server Drucker als Netzwerkdrucker eingerichtet werden.
- **Web-Mediaserver:** Mit dieser Funktion können der Internet Information Service (IIS) sowie Media-Dienste installiert werden.
- **Netzwerk:** Die Funktion Netzwerk bietet die Möglichkeit, das Netzwerk zu konfigurieren. DHCP (Dynamic Host Configuration Protocol) und DNS (Domain Name System) können z. B. über den Assistenten installiert werden.
- **Anwendungsserver:** Hierunter lassen sich u. a. Komponenten- und Terminaldienste installieren.
- **Erweitert:** Es können weitere Windows 2000-Tools, wie z. B. die Windows 2000 Support-Tools, installiert werden.

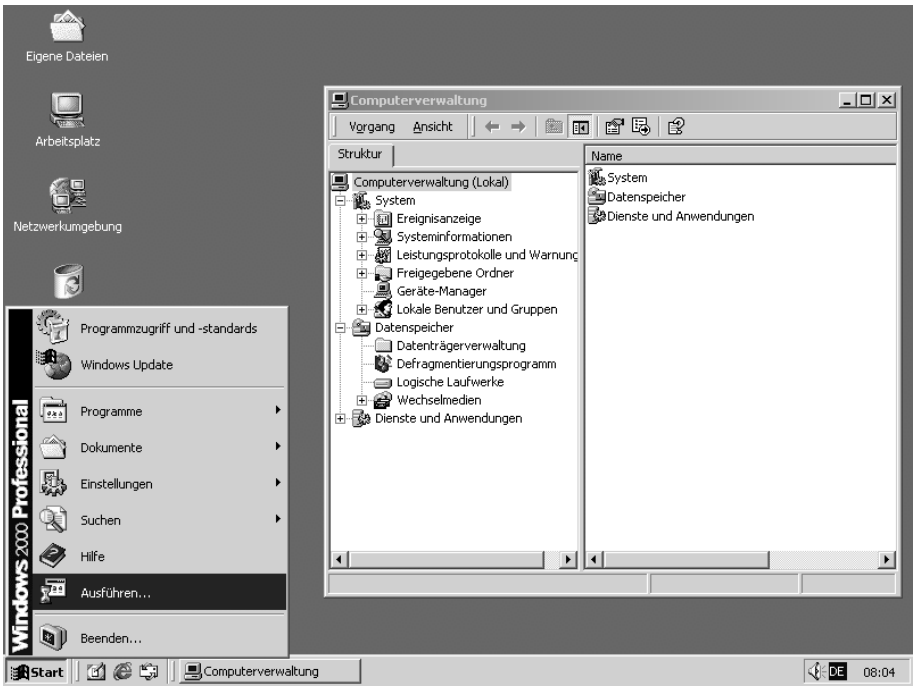
Assistent: Windows 2000 Server konfigurieren

Die optionalen Windows 2000-Komponenten sind abhängig von der Funktion, die der Server einnehmen soll. Folgende Komponenten installiert werden:

Komponente	Beschreibung
Zertifikatsdienste	Sie ermöglichen das Erstellen und Anfordern von digitalen Zertifikaten für die Authentifizierung. Mit Zertifikaten können Benutzer in nicht sicheren Netzwerken, wie z. B. dem Internet, nachprüfbar identifiziert werden.
Windows Clustering	Es ermöglicht, dass zwei oder mehr Server zusammenarbeiten, um eine Verfügbarkeit serverbasierter Anwendungen beizubehalten. Dieser Dienst steht nur unter Windows 2000 Advanced Server und Windows 2000 Datacenter Server zur Verfügung.
IIS	Es enthält die Funktionen FTP- und Webserver, die Verwaltungsschnittstelle für IIS, allgemeine IIS-Komponenten und Dokumentationen.
Verwaltungs- und Überwachungsprogramme	Sie enthalten Tools zum Überwachen und Verbessern der Netzwerkleistung.
Message Queuing	Es unterstützt Anwendungen, die Nachrichten an Warteschlangen senden. Warteschlangen haben eine ähnliche Funktion wie Caches. Sie steuern den Fluss von Daten zu Zielen und stellen sicher, dass die Nachrichten ihr Ziel erreichen.
Microsoft Indexdienst	Er ermöglicht eine dynamische Volltextsuche nach Daten, die auf dem Computer oder im Netzwerk gespeichert sind.
Microsoft Script Debugger	Er ermöglicht client- und serverseitiges Debugging von Microsoft ActiveX-Scriptmodulen.
Netzwerkdienste	Sie schließen den DHCP-Serverdienst, DNS-Serverdienst, TCP/IP und andere Netzwerkkomponenten ein.
Weitere Datei- und Druckdienste für das Netzwerk	Sie ermöglichen das Freigeben von Dateien und Druckern auf diesem Computer für Macintosh- und Unix-basierte Computer.
Remote-Installationsdienste	Sie ermöglichen eine Remoteinstallation von Windows 2000 Professional über eine Netzwerkverbindung.

Remotespeicher	Er ermöglicht die Verwendung von Bandspeichermedien als Erweiterungen von NTFS-Datenträgern.
Terminaldienste	Sie ermöglichen Windows-basierten Clients den Zugriff über Terminaldienste.

2.1.2 Windows 2000 Professional



Computerverwaltung

Viele Komponenten von Windows NT 4.0 Workstation haben in Windows 2000 Professional andere Namen erhalten. Die Bedieneroberfläche ist neu strukturiert, und die Verwaltungsprogramme sind in die *Managementkonsole (Microsoft Management Console, MMC)* integriert worden. Die Verwaltungsprogramme befinden sich unter START-EINSTELLUNGEN-SYSTEMSTEUERUNG im Ordner VERWALTUNG.

In der COMPUTERVERWALTUNG wurden die meisten für die Administration von Windows 2000 Professional notwendigen Programme zusammengefasst. Hier können z. B. lokale Benutzer und Gruppen angelegt, die Protokolle der Ereignisse eingesehen oder der Datenspeicher verwaltet werden.

Eine Windows 2000 Professional-Arbeitsstation kann problemlos in eine Windows NT 4.0-Domäne integriert werden. Die zentralen Benutzerkonten und die ihnen ggf. zugewiesenen

Sicherheitseinstellungen (Systemrichtlinien) werden von Windows 2000 Professional berücksichtigt, sodass eine gewisse Abwärtskompatibilität gewährleistet ist.

2.1.3 Windows XP

Windows XP Professional ist das aktuelle Betriebssystem von Microsoft und kann als Nachfolger von Windows 95, 98, Millennium, NT 4.0 Workstation und Windows 2000 Professional eingesetzt werden. Technisch gesehen besteht das Fundament von Windows XP Professional aus dem bewährten Windows 2000-Kernel, also den Systembestandteilen von Windows 2000. Neben Windows XP Professional wird für den privaten Nutzer Windows XP Home zur Verfügung gestellt. Die wesentlichen Unterschiede in Bezug auf den Funktionsumfang sind in der nachfolgenden Tabelle dargestellt.

Funktion	**Home**	**Professional**
Neue und einfache Benutzeroberfläche	×	×
Schutz der Systemdateien vor Änderungen (File Protection)	×	×
Heimnetzwerk-Assistent	×	×
Windows Messenger für Online-Nachrichtenaustausch	×	×
Help & Support mit automatischer Netzwerkanalyse, Geräteinventarisierung, Volltextsuche und Problemlöse-Assistenten	×	×
Notebook-Unterstützung	×	×
Drahtlose Datenverbindungen über Infrarot und Funknetzwerke	×	×
Schneller Start mit Stand-by und Ruhezustand	×	×
Internet Connection Firewall für die Abschottung des Internetzuganges	×	×
Internetdatensicherheit mit Kontrolle über Cookies und Beschränkungen auf Websites	×	×
Dateisystemunterstützung (FAT, FAT32, NTFS)	×	×

Mehrprozessorunterstützung		×
Verschlüsseltes Dateisystem		×
Zugriffsrechtevergabe auf Dateien und Ordner		×
Zentrale Administration über das Netzwerk		×
Gruppenrichtlinien		×
Ferninstallation von Software		×
Servergespeicherte Profile		×
Remote Installation Service (RIS) für die Installation über das Netzwerk		×
Anbindung an Domänen		×

Windows XP Home ist in einer vernetzten Umgebung aufgrund fehlender Sicherheitsfunktionalitäten (keine Unterstützung der Gruppenrichtlinien) für die Verarbeitung personenbezogener Daten nur begrenzt einsetzbar.

2.2 Windows Server 2003

Als Nachfolgebetriebssystem für Windows 2000 Server ist bereits Windows Server 2003 verfügbar. Die in diesem *backUP*-Magazin dargestellten Funktionen sind unter Windows Server 2003 nicht durch andere ersetzt, sondern lediglich verbessert worden. Die in diesem Magazin getroffenen Aussagen sind deshalb weitgehend übertragbar.

Die Windows Server 2003-Familie besteht aus vier Versionen:

- **Windows Standard Server** – ist ein Serverbetriebssystem, das sich für die alltäglichen Anforderungen von Organisationen jeder Größe eignet. Es werden u. a. Datei- und Druckerfreigaben, sichere Internetverbindungen, zentrale Desktopanwendungen und eine leistungsfähige Netzwerkumgebung bereitgestellt.

- **Windows Enterprise Server** – ist die geeignete Plattform, um Anwendungen, Webdienste und Infrastruktur zu entwickeln, bereitzustellen und zu sichern. Der Windows Enterprise Server steht in einer 32-Bit- und einer 64-Bit-Version zur Verfügung.
- **Windows Datacenter Server** – ist der geeignete Server für kritische Anwendungen, die höchste Skalierbarkeit und Zuverlässigkeit erfordern. Der Windows Datacenter Server steht über das Datacenter-Programm in einer 32-Bit- und einer 64-Bit-Version zur Verfügung.
- **Windows Web Server** – optimiert den Server für Webanwendungen.

Systemanforderungen der Windows Server 2003-Familie:

Anforderung	**Web Server**	**Standard Server**	**Enterprise Server**	**Datacenter Server**
empfohlene CPU-Geschwindigkeit	550 MHz	550 MHz	733 MHz	733 MHz
empfohlener minimaler Arbeitsspeicher	256 MB	256 MB	256 MB	1 GB
Speicherplatz für Installation	1,5 GB	1,5 GB	1,5 GB für x86-basierende Computer	1,5 GB für x86-basierende Computer
maximaler Arbeitsspeicher	2 GB	4 GB	32 GB für x86-basierende Computer	64 GB für x86-basierende Computer
Multiprozessorunterstützung	1 oder 2	1 oder 2	bis 8	• mindestens 8 erforderlich • maximal 32

2.3 Windows Server 2003 – Funktionenvergleichstabelle

Funktionen	verbessert in Windows Server 2003	neue Funktionen Server 2003	Web	Standard	Enterprise	Datacenter 32-Bit	Datacenter 64- Bit
.NET Framework / ASP.NET Framework		×	×	×	×	×	×
802.1x-Unterstützung (drahtloses Netzwerk)		×	×	×	×	×	×
Active Directory	×			×	×	×	×
Active Directory-Migrationstool	×			×	×	×	×
Anwendungsüberprüfung		×	×	×	×	×	×
ASP.NET		×	×	×	×	×	×
ATM-Unterstützung		×	×	×	×	×	×
Automatische Konfiguration für mehrere Netzwerkverbindungen		×	×	×	×	×	×
Automatische Systemwiederherstellung	×		×	×	×	×	×
Bandbreiteneinschränkung	×		×	×	×	×	×
Befehlszeilenprogramme		×	×	×	×	×	×
Clustering	×				×	×	×
Datei- und Druckdienste für Mac	×			×	×	×	×
Datenträgerverwaltung	×		×	×	×	×	×
DHCP mit DNS und Active Directory	×			×	×	×	×
Diagnoseprogramm für Problembehandlung		×	×	×	×	×	×
Dienste für Macintosh	×			×	×	×	×
Dienstqualität	×		×	×	×	×	×
Druckdienste für Unix	×			×	×	×	×
DualView	×		×	×	×	×	×

Funktionen	verbessert in Windows Server 2003	neue Funktionen Server 2003	Web	Standard	Enterprise	Datacenter 32-Bit	Datacenter 64- Bit
Entwicklungsmodell für verwalteten Code		×	×	×	×	×	×
Euro-Zonenunterstützung		×	×	×	×	×	×
FAT32 auf DVD-RAM		×	×	×	×	×	×
Faxdienst		×		×	×	×	×
Gemeinsame Nutzung der Internetverbindung	×			×	×	×	×
Gesamtstrukturvertrauensstellung		×	×	×	×	×	×
Gruppenrichtlinien (Bestandteil von Active Directory)	×			×	×	×	×
Hotplug-Speicher		×			×	×	×
I2O-Unterstützung		×		×	×	×	×
Indizierungsdienst	×		×	×	×	×	×
Installieren von Replikaten von Medien; Active Directory		×		×	×	×	×
Intellimirror	×		×	×	×	×	×
Internet Information Services 6.0	×		×	×	×	×	×
Internetauthentifizierungsdienst	×			×	×	×	×
Internetprotokoll v6		×	×	×	×	×	×
Internetverbindungsfirewall		×	×	×	×		
Kennwortsicherung und -wiederherstellung		×	×	×	×	×	×
Kompatibilitätsmodus		×	×	×	×	×	×
Komponentendienste	×		×	×	×	×	×
Konfigurationsprüfprogramm		×				×	×

Funktionen	verbessert in Windows Server 2003	neue Funktionen Server 2003	Web	Standard	Enterprise	Datacenter 32-Bit	Datacenter 64- Bit
Message Queuing		×	×	×	×	×	×
Metaverzeichnisdienstunterstützung		×		×	×	×	×
Microsoft Data Engine (MSDE)	×			×	×	×	×
Microsoft Managementkonsole	×		×	×	×	×	×
Migration, Unterstützung und Integration des Betriebssystems		×		×	×	×	×
Netzwerkadressübersetzung	×		×	×	×	×	×
Netzwerkbrücke	×			×	×	×	×
Netzwerklastenausgleichscluster	×		×	×	×	×	×
Non-Uniform Memory Access (NUMA)		×			×	×	×
Öffentliche Schlüsselinfrastruktur und Smartcard-Infrastruktur		×	×	×	×	×	×
Ordnerumleitung für eigene Dokumente		×	×	×	×	×	×
Plug & Play	×		×	×	×	×	×
POP3-E-Mail-Dienst	×		×	×	×	×	×
PPPoE-Verbindungen (Point-to-Point-Protokoll über Ethernet)		×	×	×	×	×	×
RAS-Anmeldeinformationen für alle Benutzer		×	×	×	×	×	×
Remotedesktop für Verwaltung	×		×	×	×	×	×
Remoteinstallation von Betriebssystemen		×	×	×	×	×	×
Remoteinstallationsdienste	×		×	×	×	×	×
Remotespeicher		×		×	×	×	×

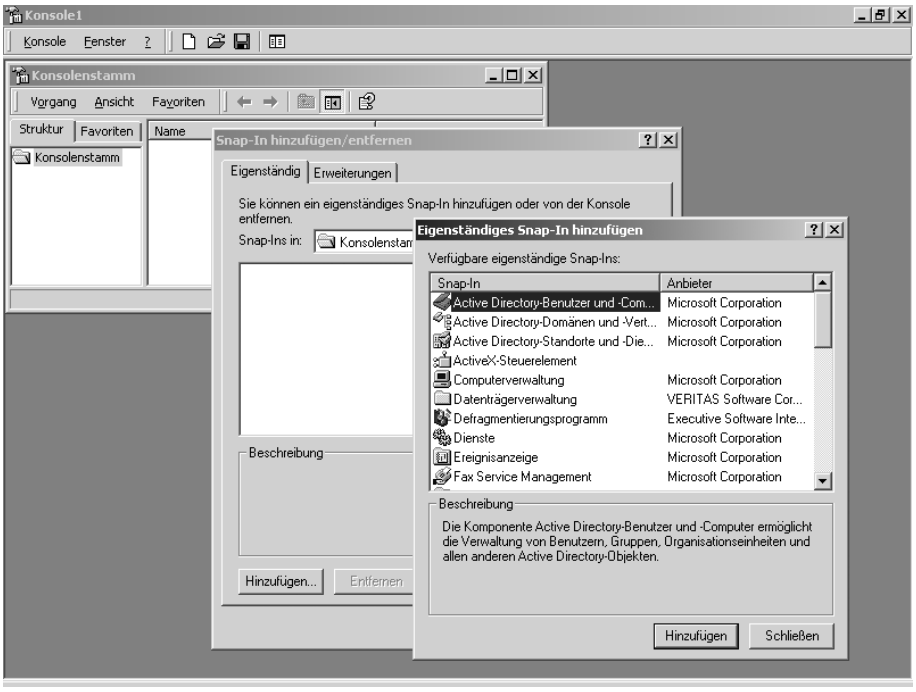
Funktionen	verbessert in Windows Server 2003	neue Funktionen Server 2003	Web	Standard	Enterprise	Datacenter 32-Bit	Datacenter 64- Bit
Remoteunterstützung	×		×	×	×	×	
Richtlinien für Softwareeinschränkung	×		×	×	×	×	×
Richtlinienergebnissatz		×	×	×	×	×	×
Routing und RAS	×		×	×	×	×	×
SAN-Unterstützung (SAN-Start)		×			×	×	×
Schattenkopie freigegebener Ordner		×	×	×	×	×	×
Server ohne Monitor		×	×	×	×	×	×
Servercluster	×				×	×	×
Serververwaltung		×	×	×	×	×	×
Sicherheitsmodus	×		×	×	×	×	×
Sicherungsprogramm	×		×	×	×	×	×
Sitzungsverzeichnis für Terminaldienste		×		×	×	×	×
Smartcard-Infrastruktur	×		×	×	×	×	×
Supportunterstützung – Microsoft Incident Submission and Management		×	×	×	×	×	×
TAPI 3.1	×		×	×	×	×	×
Terminaldienste	×			×	×	×	×
Umbenennen von Domänen		×	×	×	×	×	×
Unternehmensweite UDDI-Dienste		×	×	×	×	×	×
Unterstützung für Datenträgerkontingent	×		×	×	×	×	×
Unterstützung für Internetprotokollsicherheit		×	×	×	×	×	×

Funktionen	verbessert in Windows Server 2003	neue Funktionen Server 2003	Web	Standard	Enterprise	Datacenter 32-Bit	Datacenter 64- Bit
Unterstützung für L2TP (Layer Two Tunneling Protocol)	×		×	×	×	×	×
Unterstützung für LDAP (Lightweight Directory Access Protocol)	×		×	×	×	×	×
Unterstützung von Kerberos V5	×		×	×	×	×	×
User State Migration Tool (USMT)		×	×	×	×	×	×
Verbindungsmanager	×		×	×	×	×	×
Verschlüsselndes Dateisystem	×		×	×	×	×	×
Verteilter Dateidienst	×		×	×	×	×	×
Verwalten von Anmeldeinformationen		×	×	×	×	×	×
Virtuelle private Netzwerke	×			×	×	×	×
Voice-Over-IP-Unterstützung		×	×	×	×	×	
Volumeschattenkopie		×	×	×	×	×	×
VT-UTF8-Unterstützung für HyperTerminal		×	×	×	×	×	×
WebDAV-Umleitung		×	×	×	×	×	×
Webgärten		×	×	×	×	×	×
Wechselmedien und Remotespeicher		×	×	×	×	×	×
Wiederherstellung von Schattenkopien		×		×	×	×	×
Wiederherstellungskonsole	×		×	×	×	×	×
Windows Media-Dienste	×			×	×	×	
Windows Resource Manager (WRM)		×				×	×
Windows Script Host	×		×	×	×	×	×

Funktionen	verbessert in Windows Server 2003	neue Funktionen Server 2003	Web	Standard	Enterprise	Datacenter 32-Bit	Datacenter 64- Bit
Windows Sockets: Direkter Pfad für SAN-Netzwerke		×	×	×	×	×	×
Windows Update	×		×	×	×	×	×
Windows-Verwaltungsinstrumentations-befehlszeile (WMI)	×			×	×	×	×
Winsock Direct	×		×	×	×	×	×
Zertifikatsdienste	×		×	×	×	×	×

2.4 Die Microsoft Managementkonsole

Die unter Windows 2000 verfügbaren Verwaltungsprogramme basieren auf der *Microsoft Managementkonsole (Microsoft Management Console, MMC).*



Managementkonsole – Snap-In hinzufügen

Unter Windows 2000 Server werden die vordefinierten MMC-basierten Verwaltungsprogramme unter START-PROGRAMME-VERWALTUNG und START-EINSTELLUNGEN-SYSTEMSTEUERUNG-VERWALTUNG zur Verfügung gestellt.

Unter Windows 2000 Professional sind diese Verwaltungsprogramme standardmäßig im Ordner VERWALTUNG der Systemsteuerung verfügbar. Soll der Ordner VERWALTUNG auch unter START-PROGRAMME aufrufbar sein, dann kann er dort bei Bedarf bereitgestellt werden (START-EINSTELLUNGEN-TASKLEISTE und STARTMENÜ-ERWEITERT).

Zusätzlich zu den standardmäßig vorhandenen Verwaltungsprogrammen können mit der MMC flexible und benutzerdefinierte **Administrationsvorlagen** erstellt werden. Eine benutzerdefinierte MMC (Verwaltungskonsole) wird über so genannte *Snap-Ins* eingerichtet. Diese Snap-Ins sind als einzelne Werkzeuge (wie z. B. die Ereignisanzeige) zu verstehen. Sie können über ein Menü aufgerufen und in die benutzerdefinierte MMC eingebunden werden. Sowohl unter Windows 2000 Professional als auch unter Windows 2000 Server kann eine MMC so gespeichert werden, dass sie im Ordner VERWALTUNG des Menüs PROGRAMME verfügbar ist.

2.5 Active Directory

Der mit Windows 2000 eingeführte Verzeichnisdienst *Active Directory* bildet den Kern der Systemsicherheit. Er kann als eine Datenbank verstanden werden, in der Informationen zu Objekten gespeichert werden. Diese Objekte repräsentieren Benutzer, Gruppen, Anwendungen, Dateien sowie Drucker, Computer und weitere Peripheriegeräte.

Nach der Installation von Windows 2000 Server wird der Server **nicht** automatisch als **Domänencontroller** zur Unterstützung von Active Directory konfiguriert. Die Heraufstufung zum Domänencontroller kann entweder über den Assistenten *Windows 2000 konfigurieren* oder mit dem Befehl `dcpromo` über AUSFÜHREN durchgeführt werden. Vor Einrichtung des Domänencontrollers sollten die Namenskonventionen festgelegt werden, da sich der Name eines Domänencontrollers nachträglich nicht mehr ändern lässt.

Active Directory wird nur auf Domänencontrollern gespeichert und kann von Netzwerkanwendungen oder Diensten lediglich abgefragt werden. Sind in einer Domäne mehrere Domänencontroller vorhanden, befindet sich auf jedem eine Active Directory-Datenbank. Änderungen am Verzeichnis werden von dem Domänencontroller, von dem diese Änderungen ausge-

hen, auf die anderen Domänencontroller **innerhalb** der Domäne repliziert. Damit ist eine hohe Verfügbarkeit dieser Informationen innerhalb der Domäne gewährleistet.

Active Directory unterstützt die *Multimasterreplikation* von Verzeichnisdaten zwischen allen Domänencontrollern der Domäne. Da einige Änderungen im Multimasterbetrieb jedoch wenig sinnvoll sind, werden solche Änderungsanforderungen nur von einem Domänencontroller, dem so genannten *Betriebsmaster*, akzeptiert.

Das unter Windows NT Server 4.0 verwendete Modell des *Primären Domänencontrollers* (PDC) und des *Backup Domänencontrollers* (BDC) wird nicht mehr unterstützt. Unter Windows 2000 gibt es „nur“ noch einen oder mehrere Domänencontroller (DC).

Active Directory bietet Sicherheitsfunktionen wie die **Anmeldeauthentifizierung** und den **gesteuerten** Zugriff auf Verzeichnisobjekte. So können Administratoren mit einer einzigen Netzwerkanmeldung die Verzeichnisdaten und die Verzeichnisstruktur in der gesamten Domänenstruktur verwalten. Autorisierte Netzwerkbenutzer können im gesamten Netzwerk auf die benötigten Ressourcen zugreifen.

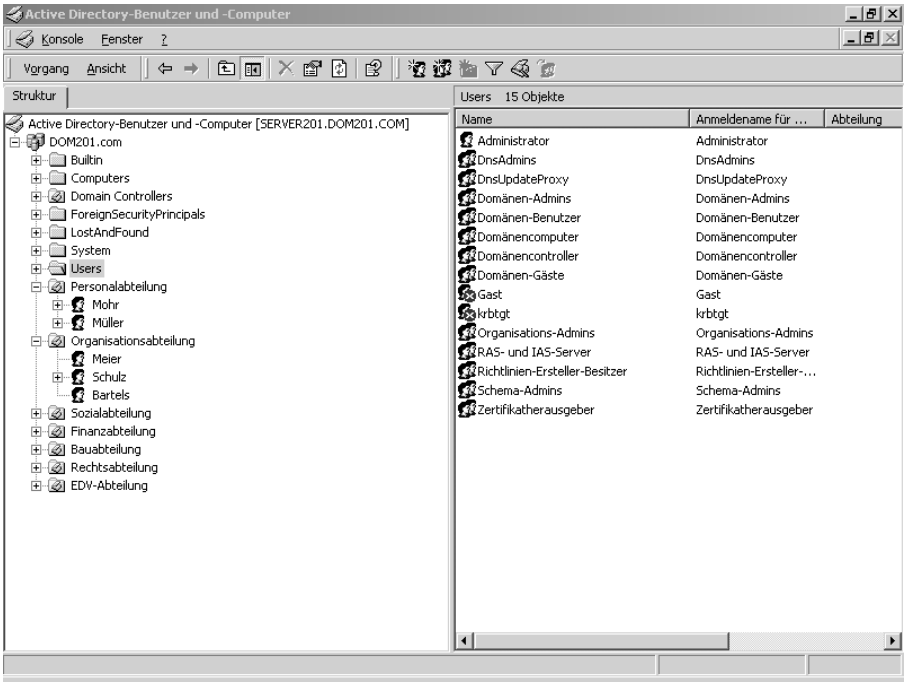
Das Lightweight Directory Access Protocol (LDAP) wird als primäres Zugriffsprotokoll für Active Directory verwendet. Darüber hinaus wird für eine im Active Directory durchgeführte Informationsabfrage als Voraussetzung das DNS (Domain Name System, siehe Kapitel 4) benötigt. DNS wird automatisch installiert, wenn ein Server zum Domänencontroller heraufgestuft wird. Das gilt allerdings nicht, wenn Windows 2000 einen vorhandenen DNS-Server für die betreffende Domäne erkennt. Bei der Installation von DNS auf einem Server muss eine statische IP-Adresse für den Server angegeben werden. Für die Netzwerkkommunikation ist es unverzichtbar, dass auf den Clients die IP-Adresse des zuständigen DNS-Servers eingetragen wird.

2.5.1 Active Directory-Benutzer und -Computer

Active Directory-Benutzer und -Computer ist eine MMC-basierte Verwaltungskonsole zum Verwalten und Veröffentlichen von Verzeichnisinformationen.

Die folgende Tabelle enthält allgemeine Aufgaben, die mit dem Verwaltungsprogramm *Active Directory-Benutzer und -Computer* ausgeführt werden können. Benutzer können der Tabelle entnehmen, wo diese Aufgaben bei der Verwendung der in Windows NT Server 4.0 enthaltenen Verwaltungsprogramme ausgeführt werden.

Aufgaben	**Windows NT 4.0**
Verwalten von Benutzerkonten	Benutzer-Manager
Verwalten von Gruppen	Benutzer-Manager
Verwalten von Computerkonten	Server-Manager
Hinzufügen eines Computers zu einer Domäne	Server-Manager
Verwalten von Kontorichtlinien	Benutzer-Manager
Verwalten von Benutzerrechten	Benutzer-Manager
Verwalten von Überwachungsrichtlinien	Benutzer-Manager



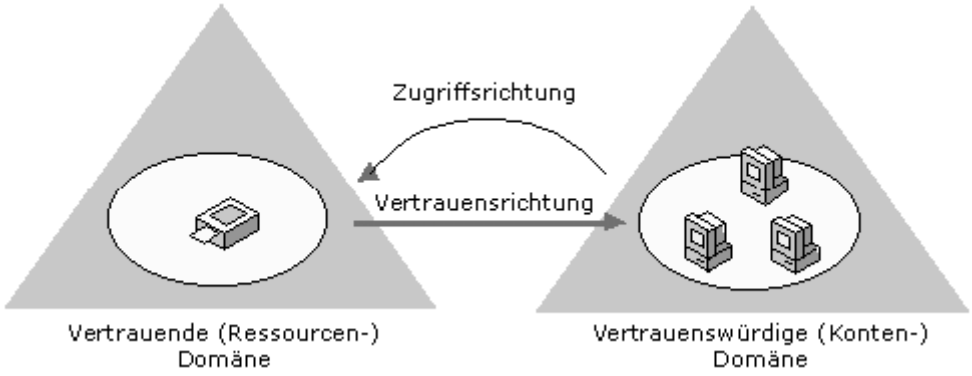
Active Directory-Benutzer und -Computer

2.5.2 Active Directory-Domänen und -Vertrauensstellungen

Mit dem Verwaltungsprogramm *Active Directory-Domänen und -Vertrauensstellungen* können Vertrauensstellungen zwischen Domänen (siehe Kapitel 3) administriert und der Betriebsmodus der Domäne definiert werden.

Es wird zwischen zwei Betriebsmodi in einer Domäne unterschieden. Im gemischten Modus, der die Standardeinstellung für Windows 2000-Domänencontroller darstellt, können Windows NT- und Windows 2000-Domänencontroller in einer Domäne vorhanden sein. Wenn alle NT-Domänencontroller aus der Domäne entfernt oder auf Windows 2000 umgestellt wurden, kann die Betriebsmodus-Einstellung zum einheitlichen Modus geändert werden. Erst im einheitlichen Modus können innerhalb einer Domäne **alle** neuen Verzeichnisfunktionen von Windows 2000 (wie z. B. universelle oder verschachtelte Gruppen) genutzt werden.

Eine **Vertrauensstellung** ist eine Beziehung zwischen zwei Domänen, durch die Benutzer einer Domäne von einem Domänencontroller authentifiziert werden können, der sich in einer anderen Domäne befindet. Eine Vertrauensstellung zwischen Domänen wird immer nur zwischen zwei Domänen aufgebaut: der vertrauenden und der vertrauenswürdigen Domäne.



Vertrauensstellung

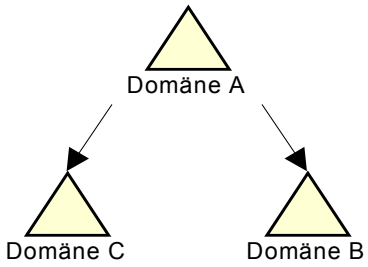
Active Directory unterstützt zwei Formen der Vertrauensstellungen:

- unidirektionale, nicht transitive (nicht vererbbare) Vertrauensstellung – (one-way),
- bidirektionale, transitive (vererbbare) Vertrauensstellung – (two-way).

Unidirektionale, nicht transitive Vertrauensstellung (one-way)

Unter Windows 2000 können (aus Kompatibilitätsgründen zu Windows NT 4.0 und zur Einrichtung von Vertrauensstellungen zwischen unterschiedlichen Domänengesamtstrukturen (siehe Tz. 3.3)) unidirektionale, nicht transitive Vertrauensstellungen eingerichtet werden. Eine unidirektionale Vertrauensstellung ist eine einseitige Beziehung, in der z. B. Domäne A Domäne B als vertrauenswürdig anerkennt. Alle unidirektionalen Vertrauensstellungen sind

nicht transitiv, d. h., eine Vertrauensbeziehung wird nicht von einer Vertrauensstelle zu anderen Vertrauensstellen durchgeleitet.



Unidirektionale Vertrauensstellung (one-way)

Besteht z. B. eine unidirektionale Vertrauensstellung zwischen Domäne A und Domäne B und eine weitere unidirektionale Vertrauensstellung zwischen Domäne A und Domäne C, dann bestehen folgende Zugriffsrichtungen:

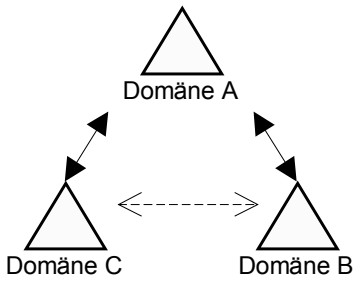
- A vertraut C. C kann auf Ressourcen von A zugreifen.
- A vertraut B. B kann auf Ressourcen von A zugreifen.
- B und C vertrauen nicht A. A kann nicht auf Ressourcen von B und C zugreifen.
- B und C vertrauen sich gegenseitig nicht. Sie können nicht auf die Ressourcen des anderen zugreifen.

Bei der Aktualisierung von Windows NT auf Windows 2000 bleiben alle vorhandenen Windows NT-Vertrauensstellungen bestehen.

Bidirektionale, transitive Vertrauensstellung (two-way)

Alle Vertrauensstellungen zwischen Domänen **innerhalb** einer **Domänengesamtstruktur** unter Windows 2000 sind standardmäßig bidirektionale und transitive Vertrauensstellungen. Wird z. B. eine Vertrauensstellung zwischen Domäne A und Domäne B eingerichtet, dann wird automatisch eine bidirektionale, transitive Vertrauensstellung erstellt. Bidirektional bedeutet, dass beide Domänen sowohl vertrauende als auch vertraute Domänen sind, d. h., Domäne A vertraut Domäne B und Domäne B vertraut Domäne A.

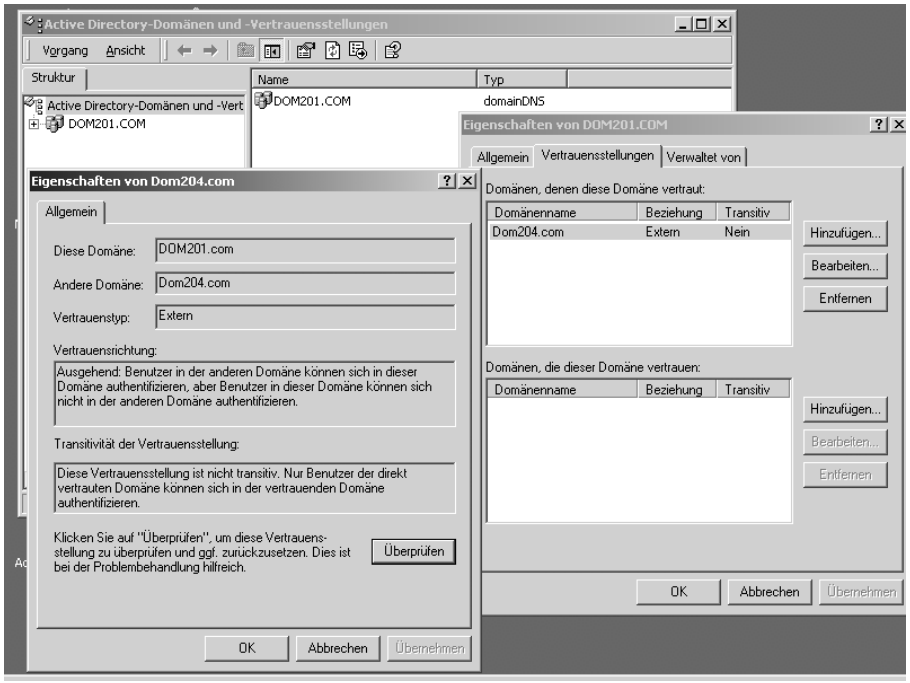
Transitiv bedeutet, dass eine Vertrauensbeziehung von einer Vertrauensstelle zu anderen Vertrauensstellen **durchgeleitet** wird.



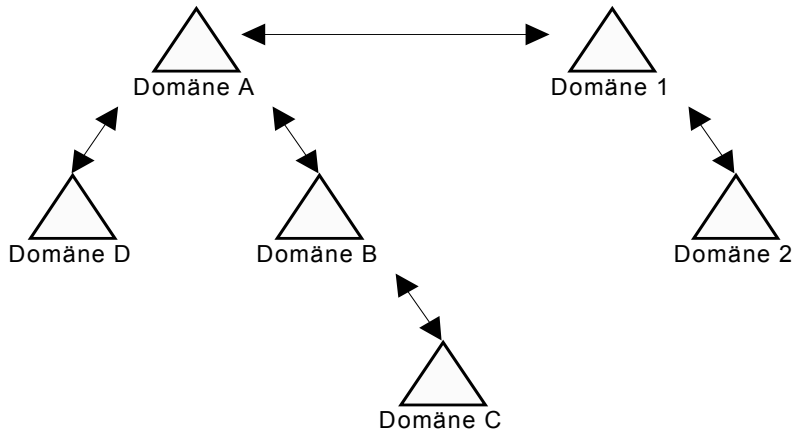
Bidirektionale, transitive Vertrauensstellung (two-way)

Besteht z. B. eine bidirektionale, transitive Vertrauensstellung zwischen Domäne A und Domäne B und eine weitere bidirektionale Vertrauensstellung zwischen Domäne A und Domäne C, dann bestehen folgende Zugriffsrichtungen:

- A und B vertrauen sich gegenseitig. Ressourcen von A und B stehen im Zugriff.
- A und C vertrauen sich gegenseitig. Ressourcen von A und C stehen im Zugriff.
- B kann aufgrund der gegenseitigen Vertrauensstellung zwischen A und B sowie A und C auch auf Ressourcen von C zugreifen. Das Gleiche gilt für C für den Zugriff auf die Ressourcen von B.



Active Directory-Domänen und -Vertrauensstellungen



Vertrauensstellungen in einer Domänengesamtstruktur

Jedes Mal, wenn eine neue untergeordnete Domäne erstellt wird, wird zwischen der neuen untergeordneten und der übergeordneten Domäne **automatisch** eine weitere bidirektionale, transitive Vertrauensstellung eingerichtet.

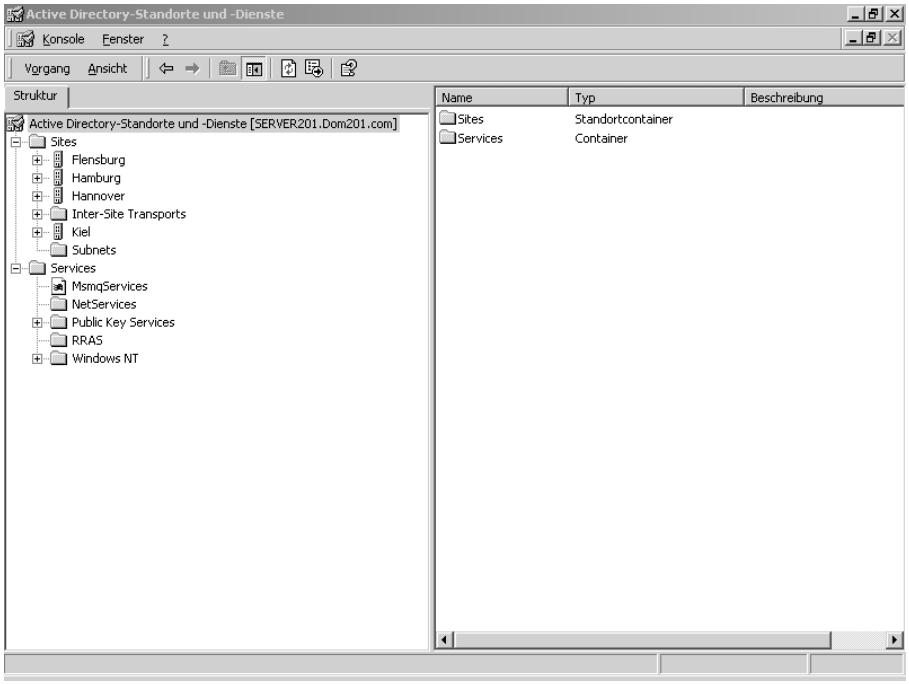
Auf diese Weise können sich transitive Vertrauensstellungen in einer wachsenden Domänenstruktur weiter **fortpflanzen**, sodass Benutzer in einer Domänengesamtstruktur in jeder beliebigen Domäne authentifiziert werden können.

2.5.3 Active Directory-Standorte und -Dienste

Mit *Active Directory-Standorte und -Dienste* können Informationen zur **physischen Struktur** des Netzwerkes (siehe Kapitel 5) im Active Directory bereitgestellt werden. Anhand dieser Informationen kann Active Directory festlegen, auf welche Weise Verzeichnisinformationen repliziert und Dienstanforderungen verarbeitet werden.

Grundsätzlich ist ein Domänencontroller für die **Veröffentlichung von Verzeichnisinformationen** und die **Beantwortung von Dienstanforderungen** ausgelegt. Im Active Directory können aber auch Dienste zugewiesen werden. Clients können auf diese Dienste zugreifen, ohne dass sie wissen müssen, auf welchem Domänencontroller der entsprechende Dienst ausgeführt wird.

Der Knoten für die Dienste (Services) wird von *Active Directory-Standorte und -Dienste* zunächst nicht angezeigt. Er kann jedoch über ANSICHT-DIENSTKNOTEN ANZEIGEN in die Managementkonsole aufgenommen werden. Standardmäßig wird eine bestimmte Gruppe von Diensten im Active Directory bereitgestellt. Die Gruppe kann gemäß den Anforderungen der Netzwerkumgebung erweitert werden.



Active Directory-Standorte und -Dienste

Um die Replikation der Active Directory-Datenbank zwischen mehreren Domänencontrollern in einer Domänengesamtstruktur effizient zu organisieren, können Computer (Server und Clients) in einem so genannten Standort zusammengefasst werden. Innerhalb eines Standortes werden dann die Verzeichnisinformationen häufiger repliziert. Das garantiert, dass alle Domänencontroller innerhalb eines Standortes stets auf die aktuellen Verzeichnisinformationen zugreifen können. Durch ein größeres Replikationsintervall zwischen den verschiedenen Standorten verringert sich der Datenaustausch, und das Netzwerk wird nicht unnötig belastet.

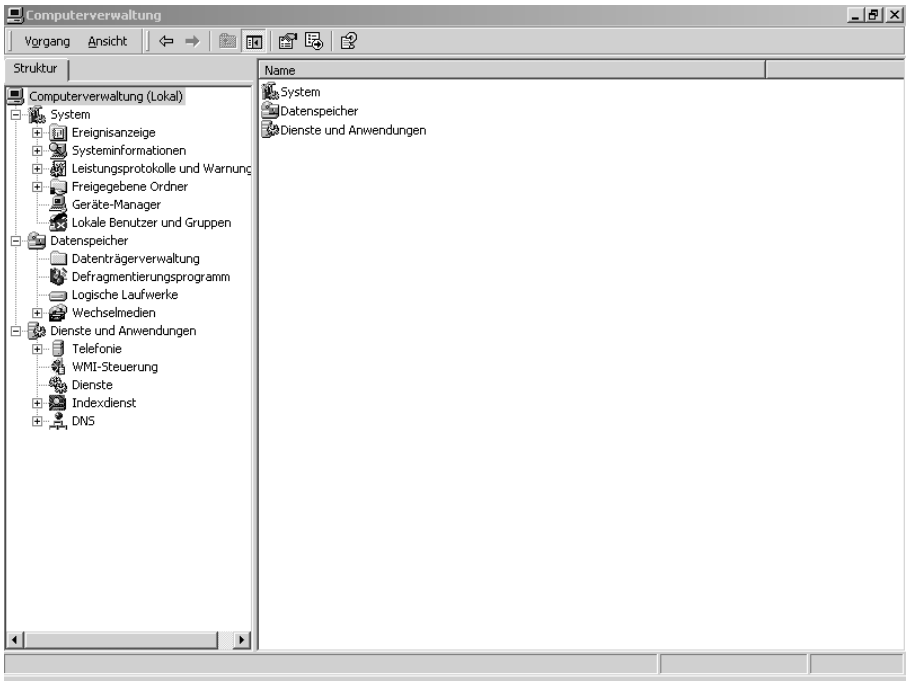
2.6 Computerverwaltung

In der *Computerverwaltung* werden mehrere Windows 2000-Verwaltungsprogramme in einer einzelnen Konsolenstruktur (MMC) vereint.

Mit der Computerverwaltung können folgende Aktionen durchgeführt werden:

- Überwachen von Systemereignissen, z. B. Anmeldezeiten und Anwendungsfehlern,
- Erstellen und Verwalten von Freigaben,
- Anzeigen einer Liste von Benutzern, die mit einem lokalen Computer bzw. einem Remotecomputer verbunden sind,

- Starten und Beenden von Systemdiensten, z. B. Taskplaner und Spooler,
- Festlegen von Eigenschaften für Speichergeräte,
- Anzeigen von Gerätekonfigurationen und Hinzufügen neuer Gerätetreiber,
- Verwalten von Serveranwendungen und -diensten, z. B. DNS-Dienst (Domain Name System) oder DHCP-Dienst (Dynamic Host Configuration Protocol).



Computerverwaltung

2.7 Weitere (Sicherheits-)Funktionen im Überblick

- **Active Directory-Schnittstellen**

Die Active Directory-Schnittstellen umfassen ein Verzeichnisdienstmodell und eine Gruppe von COM-Schnittstellen. Über diese Schnittstellen können Anwendungen für Windows 95, Windows 98, Windows NT und Windows 2000 auf verschiedene Netzwerkverzeichnisdienste zugreifen, beispielsweise auf Active Directory. Es kann als SDK (Software Development Kit) bezogen werden.

- **Asynchronous Transfer Mode (ATM)**

  Dieses verbindungsorientierte Hochgeschwindigkeitsprotokoll dient zur Übertragung von Datenverkehr über ein Netzwerk. Dieses Protokoll steht sowohl bei LANs als auch bei WANs zur Verfügung. Mit ATM kann das Netzwerk gleichzeitig eine Vielzahl unterschiedlicher Arten von Datenverkehr transportieren: Sprache, Daten, Bilder und Videos.

- **Datenträgerverwaltung**

  Die Verwaltung der Datenträger umfasst zahlreiche neue Funktionen, insbesondere die Unterstützung dynamischer Datenträger sowie die Online-Datenträgerverwaltung. Des Weiteren können über die Funktion Datenträgerkontingente auf einem NTFS-Dateisystem Benutzern Speicherplatzkapazitäten zugewiesen bzw. begrenzt und überwacht werden.

- **DHCP (Dynamic Host Configuration Protocol)**

  DHCP weist den Computern oder anderen Ressourcen, die mit einem IP-Netzwerk verbunden sind, automatisch eine IP-Adresse zu.

- **EFS (Encrypting File System)**

  Mit EFS werden die vorhandenen Zugriffssteuerungen auf Dateien und Ordner ergänzt. Sie können vom Benutzer verschlüsselt verwaltet werden. Das EFS wird als integrierter Systemdienst ausgeführt (siehe Tz. 8.6).

- **Gruppenrichtlinie (Bestandteil von Active Directory)**

  Über die Gruppenrichtlinien können die für Benutzer und Computer zulässigen Vorgänge und Einstellungen definiert werden. Die richtlinienbasierte Verwaltung vereinfacht Aufgaben wie die Aktualisierung des Betriebssystems, Anwendungsinstallationen, die Verwaltung von Benutzerprofilen und Sperrungen der Desktop-Funktionen.

- **IntelliMirror**

  Mit IntelliMirror wird die Konfiguration der Clients unter Windows 2000 Professional zentral gesteuert. Mithilfe dieser Richtlinie wird der Windows 2000 Professional-Desktop automatisch bei jedem Anmelden eines Benutzers gemäß seinen speziellen Anforderungen konfiguriert, unabhängig davon, auf welchem Computer sich der Benutzer anmeldet. IntelliMirror umfasst die Funktionen Verwaltung der Benutzerdaten, Installieren und Warten von Software sowie Verwalten der Benutzereinstellungen.

- **IPSec**

  IPSec gilt als Industriestandard für die Verschlüsselung von TCP/IP-Verkehr. Mit diesem Protokoll können die Sicherheit für die Kommunikation innerhalb eines Intranets gewährleistet und sichere VPN (virtuelles privates Netzwerk)-Lösungen über das Internet realisiert werden.

- **Kerberos V5-Protokoll**

  Kerberos V5 ist ein Netzwerk-Authentifizierungsprotokoll, das als Industriestandard gilt. Mit der Unterstützung von Kerberos V5 können dem Benutzer über einen einzigen Anmeldevorgang Zugriffe auf Windows 2000 Server-basierte Ressourcen und auch auf andere Umgebungen gewährt werden, in denen dieses Protokoll unterstützt wird. Die Unterstützung von Kerberos V5 umfasst außerdem die gegenseitige Authentifizierung. Sowohl der Client als auch der Server müssen eine Authentifizierung vornehmen. Die Kerberos V5-Authentifizierung wird bei der Installation von Windows 2000 Server automatisch aktiviert.

- **LDAP-Unterstützung (Lightweight Directory Access Protocol)**

  LDAP ist ein für TCP/IP-Netzwerke entwickeltes Kommunikationsprotokoll. Das LDAP-Protokoll legt fest, auf welche Weise Clients auf das Active Directory zugreifen, um Verzeichnisinformationen nutzen zu können.

- **Message Queuing**

  Message Queuing gewährleistet die zuverlässige Zustellung von Nachrichten, effizientes Routing, Sicherheit und prioritätsbasierte Nachrichtenübermittlung. Es ermöglicht, dass verteilte Anwendungen, die zu verschiedenen Zeitpunkten ausgeführt werden, über heterogene Netzwerke und mit Computern kommunizieren können, die sich im Offlinemodus befinden.

- **Netzwerkadressübersetzung**

  Mit der Netzwerkadressübersetzung werden die intern verwalteten IP-Adressen den externen Netzwerken gegenüber verborgen. Hierzu werden die privaten internen Adressen in öffentliche externe Adressen übersetzt. Die interne Netzwerkstruktur wird verborgen, sodass das Risiko eines Angriffs auf die internen Systeme reduziert wird.

- **Remoteinstallationsdienste**

  Mit den Remoteinstallationsdiensten kann Windows 2000 Professional unbeaufsichtigt und zentral installiert werden. Die Zielclients müssen entweder Remotebootvorgänge mittels PXE (Pre-Boot eXecution Environment)-ROM unterstützen, oder sie müssen mit einer Remotestartdiskette gestartet werden. Die Installation mehrerer Clients wird beträchtlich vereinfacht.

- **Starten im abgesicherten Modus**

  Im abgesicherten Modus kann Windows 2000 mit einem minimalen Satz von Treibern und Diensten gestartet werden, um die Probleme mit Treibern und anderen Komponenten diagnostizieren zu können.

- **Terminaldienste**

  Mithilfe der Terminaldienste greifen die Benutzer über Windows-Clients auf Programme zu, die auf dem Server ausgeführt werden. Die Benutzer können beispielsweise einen virtuellen Windows 2000 Professional-Desktop und 32-Bit-Windows-Anwendungen nutzen, die lokal auf der vorhandenen Hardware nicht ausgeführt werden könnten. Die Terminaldienste ermöglichen diese Funktion sowohl für Windows-Clients als auch für Clients mit anderen Betriebssystemen. Bei Systemen ohne Windows wird die Add-On-Software von Citrix Systems benötigt.

- **Windows Scripting Host**

  Mithilfe von Windows Scripting Host (WSH) können bestimmte Aufgaben, wie z. B. das Erstellen einer Verknüpfung oder das Aufbauen und Trennen einer Verbindung zu einem Netzwerkserver, über die Erstellung von Skripten automatisiert werden. Der WSH ist sprachenunabhängig, d. h., die Skripte können mit den verbreiteten Skriptsprachen, wie Visual Basic Scripting Edition oder Java-Script, erstellt werden.

- **Zertifikatsdienste**

  Mithilfe der Zertifikatsdienste und den Programmen zur Zertifikatsverwaltung kann eine eigene Infrastruktur öffentlicher Schlüssel verwaltet werden. Eine Infrastruktur öffentlicher Schlüssel ermöglicht die Implementierung von Standardtechnologien, darunter Smartcard-Anmeldefunktionen, Clientauthentifizierung über SSL (Secure Sockets Layer) und TLS (Transport Layer Security), sichere E-Mail, digitale Signaturen und sichere Verbindungen unter Verwendung der IP-Sicherheit.

2.8 Verwaltungsprogramme

Mit der Standardinstallation von Windows 2000 Server und Professional werden nicht alle Verwaltungsprogramme automatisch installiert. Unter PROGRAMME-VERWALTUNG werden nur die für die „allgemeine“ Administration von Windows 2000 installierten Verwaltungsprogramme aufgeführt. Sofern „spezielle“ administrative Aufgaben wahrzunehmen sind, können weitere Verwaltungsprogramme nachinstalliert werden.

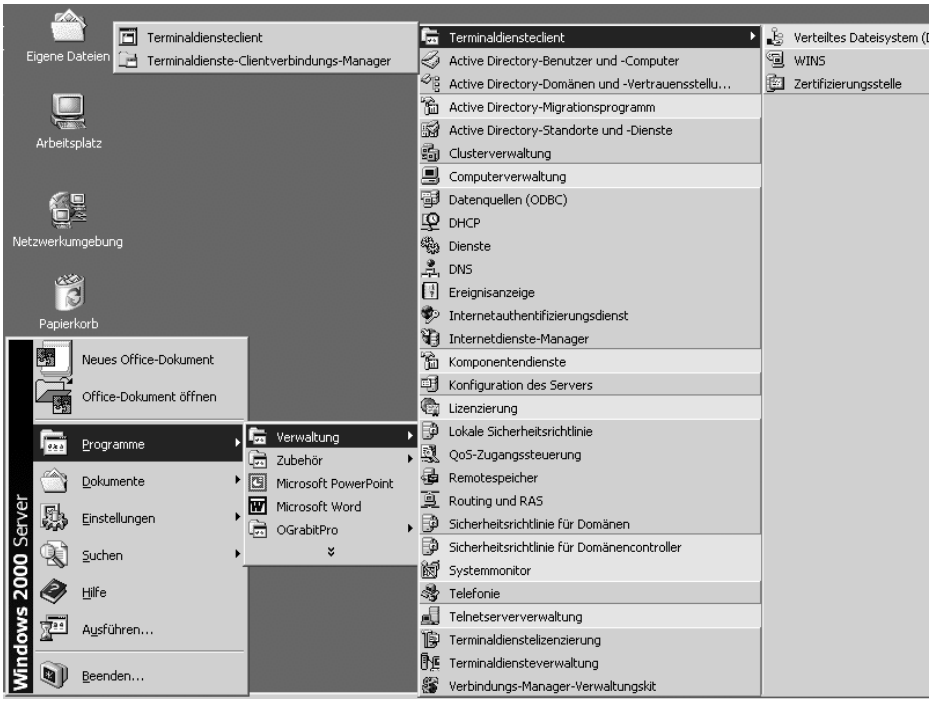
Windows 2000-Verwaltungsprogramme installieren!

1. *Zum Installieren der Windows 2000-Verwaltungsprogramme öffnen Sie den Ordner I386 auf der Windows 2000 Server-CD und doppelklicken dann auf die Datei adminpak.msi.*

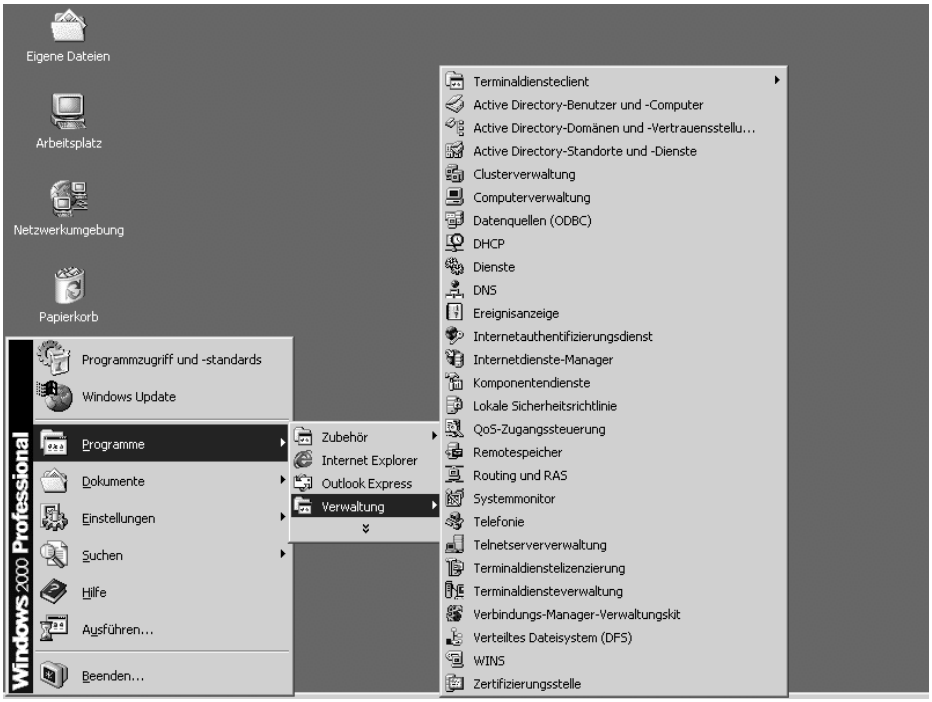
2. *Sofern adminpak.msi sich bereits auf der Festplatte befindet, geben Sie unter AUSFÜHREN* `adminpak.msi` *ein oder suchen zunächst nach dieser Datei.*

3. *Folgen Sie den Anweisungen des Assistenten zum Installieren der Windows 2000-Verwaltungsprogramme.*

4. *Nach der Installation der Windows 2000-Verwaltungsprogramme können Sie auf alle Serververwaltungsprogramme zugreifen, indem Sie auf START-PROGRAMME-VERWALTUNG klicken.*



Verwaltungsprogramme unter Windows 2000 Server

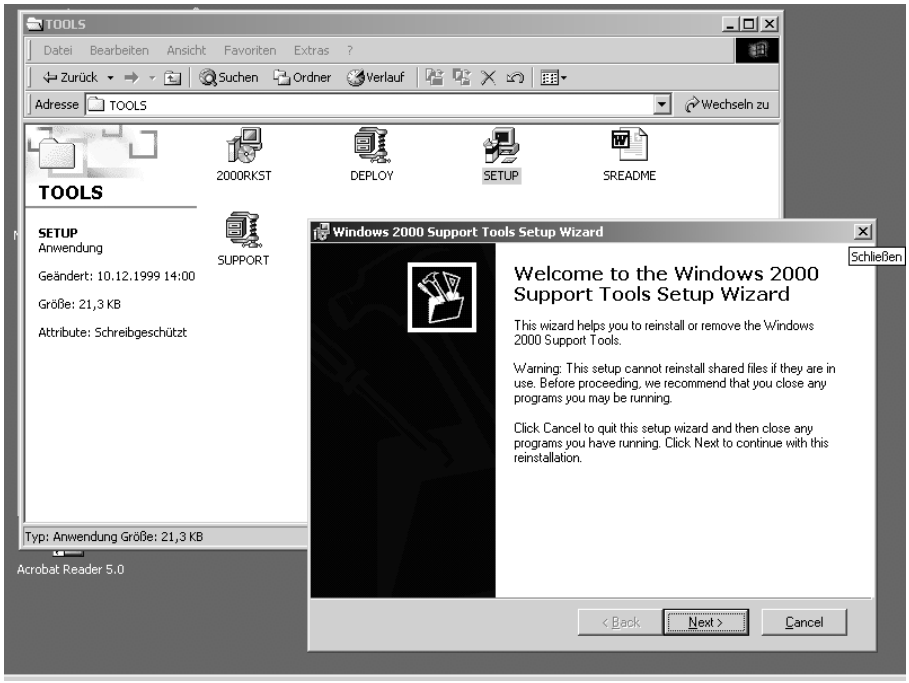


Verwaltungsprogramme unter Windows 2000 Professional

Die Installation von *Adminpak* auf dem Client hat den Vorteil, dass auch serverbasierte Administrationsaufgaben, wie z. B. die Administration der Benutzerkonten, über das Active Directory durchgeführt werden können. Nach der Installation von *Adminpak* werden die Verwaltungsprogramme jedoch nur zum Teil in die Oberfläche unter PROGRAMME-VERWALTUNG integriert. Ein weiterer Teil wird als Snap-In über die Managementkonsole zur Verfügung gestellt.

2.9 Windows 2000 Resource Kit und Support-Tools

Das *Microsoft Windows 2000 Resource Kit* ist die offizielle Quelle für technische **Hintergrundinformationen** zum Betriebssystem Windows 2000. Es bietet System- und Netzwerkadministratoren umfassende Unterstützung bei der Konfigurierung, Verwaltung, Optimierung und Problembehandlung von Windows 2000. Die Tools werden direkt von den Microsoft-Produktentwicklungsteams zur Verfügung gestellt (siehe Anhang).



Support-Tools, Windows 2000-CD-Satz

Das *Windows 2000 Professional Resource Kit* umfasst folgende Elemente:

- Das Handbuch zum *Windows 2000 Professional Resource Kit* in gedruckter Form mit Informationen zu den Kerntechnologien in Windows 2000 Professional.
- Die Resource Kit-Begleit-CD umfasst:
  - Das Handbuch zum Microsoft Windows 2000 Professional Resource Kit in Online-form.
  - Einen Teil der Resource Kit--Tools.
  - Dokumentationen zu den Tools, zur Registrierung, zu den Leistungsindikatoren, zu den Fehler- und Ereignismeldungen sowie zu den Gruppenrichtlinieneinstellungen.

Das *Windows 2000 Server Resource Kit* umfasst folgende Elemente:

- Die Handbücher zum *Windows 2000 Server Resource Kit* in gedruckter Form, die aus sieben Bänden mit Informationen zu den Technologien in Windows 2000 Server bestehen.

- Die Resource Kit-Begleit-CD enthält:
  - Sämtliche Resource Kit-Handbücher in Onlineform, einschließlich des Handbuchs zum *Microsoft Windows 2000 Professional Resource Kit*.
  - Sämtliche Resource Kit-Tools (mehr als 200 Tools).
  - Dokumentationen zu den Tools, zur Registrierung, zu den Leistungsindikatoren, zu den Fehler- und Ereignismeldungen sowie zu den Gruppenrichtlinieneinstellungen.

Der **Windows 2000-CD-Satz** beinhaltet einen Teil des Windows 2000 Resource Kit, die *Windows 2000 Support-Tools*. Sie enthalten den

- Microsoft Windows 2000 Server Resource Kit Deployment Planning Guide in Onlineform sowie
- ca. 50 der Resource Kit-Tools.

2.10 Sicherheitscheck

- *Der Einsatz von Windows 2000 ist abhängig von der eingesetzten Hardware. Überprüfen Sie vor der Installation die **Systemanforderungen**.*
- ***Windows XP Home** ist für einen sicheren Einsatz im Netzwerk nicht geeignet.*
- *Die **Microsoft Managementkonsole** dient als flexibles Administrationswerkzeug.*
- *Das **Verständnis** der Funktionsweise des Active Directory ist Grundlage für die richtige Umsetzung von technischen Sicherheitsmaßnahmen.*
- *Erst mit der Installation eines **Domänencontrollers** wird das Active Directory eingerichtet.*
- *Das **Adminpak** und das **Resource Kit** bzw. die **Support -Tools** beinhalten nützliche Administrationshilfen.*

3 Grundlagen Windows 2000

In diesem Kapitel erfahren Sie,

- was bei der Migration von Windows NT 4.0 auf Windows 2000 Server zu beachten ist,
- welche Migrationsverfahren möglich sind,
- welche Domänenkonzepte von Windows 2000 unterstützt werden,
- was unter den Betriebsmasterfunktionen zu verstehen ist,
- welche Bedeutung der Domänenmodus hat und
- welche Funktionen für die Datenträgerverwaltung zur Verfügung stehen.

3.1 Migration von Windows NT 4.0 Server auf Windows 2000 Server

Die Auswahl der geeigneten **Migrationsstrategie** muss sich an einer Reihe von Faktoren orientieren, die für den eigentlichen Prozess der Migration und dessen Verlauf entscheidend sind. Beispielsweise unterscheiden sich die Anforderungen einer zentralen Organisation mit wenigen Mitarbeitern von denen einer weit verzweigten Organisation. Auch die Größe und Komplexität der Umgebung sind entscheidend und müssen berücksichtigt werden. Die vorhandene Hardware und die Netzwerkinfrastruktur beeinflussen den Vorgang außerdem. Schließlich müssen die Desktop-Umgebung und die Applikationen im neuen Betriebssystem stabil einsatzfähig sein.

Folgendes sollten Sie bei der Planung einer Migration beachten:

- *Legen Sie fest, ob ein Upgrade einer bestehenden Windows NT 4.0-Domäne oder ein Neuaufbau einer Windows 2000-Domäne durchgeführt werden soll.*
- *Überprüfen Sie vor dem Installieren von Windows 2000, ob Ihre Hardware in der Hardwarekompatibilitätsliste (Hardware Compatibility List, HCL) für Windows 2000 enthalten ist.*
- *Eine Kopie der HCL finden Sie in der Datei hcl.txt im Ordner SUPPORT auf der Windows 2000-CD. Die aktuelle Version der HCL ist auf der Microsoft-Webseite abrufbar.*

- *Führen Sie eine Anwendungs- und Hardware-Kompatibilitätsprüfung mit dem Windows 2000 Readiness Analyzer durch. Das Tool können Sie von der Webseite <www.microsoft.com/germany/ms/windows2000/upgrade/default.htm> herunterladen.*
- *Legen Sie den Namensraum für die Windows 2000-Domäne fest.*
- *Prüfen Sie, inwieweit sich die Netzwerkinfrastruktur (IP-Adressen, Domänen- und DNS-Namen) durch die Installation einer Windows 2000-Domäne verändert.*
- *Legen Sie eine Back-up-Strategie für das Active Directory fest.*
- *Definieren Sie vor der Übernahme von Benutzer- und Gruppenkonten aus der Windows NT 4.0-Domäne die Struktur des Active Directory.*
- *Beachten Sie dabei die neuen Windows 2000-Sicherheitsfunktionalitäten, wie z. B. die Gruppen- und Sicherheitsrichtlinien.*
- *Berücksichtigen Sie, dass die Administratoren über ausreichendes Know-how für eine ordnungsgemäße Migration und Administration der Windows 2000-Systeme verfügen.*

Sofern Sie bereits über eine Windows 2000-Installations-CD verfügen, finden Sie den *Windows 2000 Readiness Analyzer* im Ordner \I386. Sie können das Programm starten, indem Sie unter AUSFÜHREN den Befehl `<CD-ROM-Laufwerk:\I386\Winnt32 /checkupgradeonly>` eingeben. Der Befehl `Winnt32 /?` listet weitere Parameter für die Einrichtung oder Aktualisierung auf.

3.1.1 Migrationsverfahren

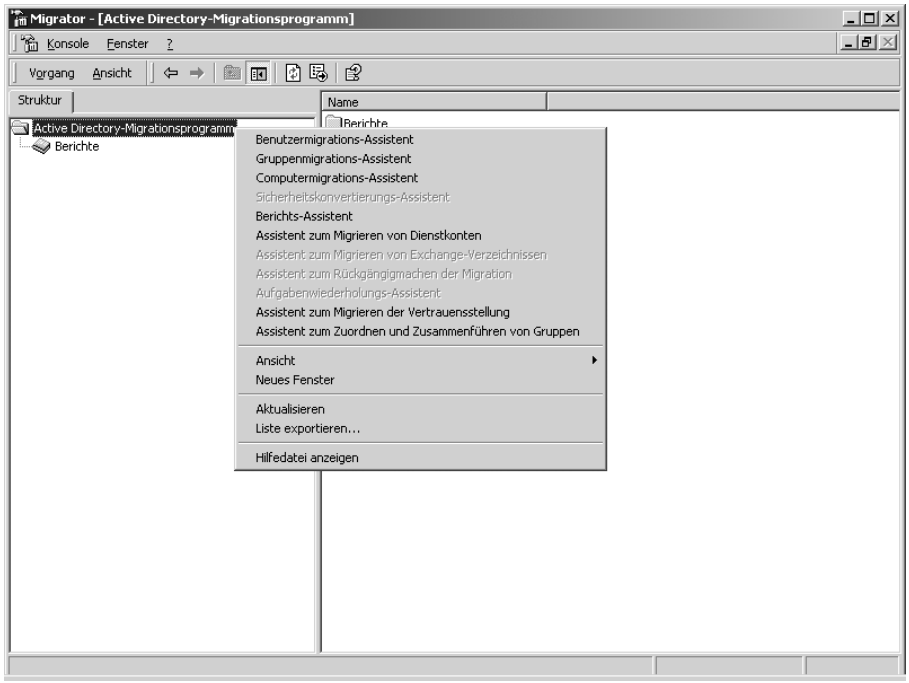
Für eine optimale **Migrationsstrategie** gibt es kein Patentrezept. Es können grundsätzlich zwei Methoden angewandt werden. Bei einer **Aktualisierung** werden die vorhandenen Windows NT-Server direkt auf Windows 2000 umgestellt. Diese Methode bietet sich für kleinere Organisationen mit wenigen Servern an, wenn die Domäneninfrastruktur mit ihren Benutzern, Gruppen und sonstigen Ressourcen beibehalten werden soll. Für eine Aktualisierung wird keine zusätzliche Hardware benötigt, und es muss kein Migrationsprogramm eingesetzt werden. Diese Migrationsmethode birgt jedoch ein hohes Risikopotenzial, da sich Probleme während der Aktualisierung direkt auf die Domäne und deren Benutzer auswirken. Damit während einer Aktualisierung keine Daten verloren gehen, sollte zuvor eine vollständige Sicherung aller Server durchgeführt werden und ein synchronisierter Windows NT-

Backupdomänencontroller (BDC) vorhanden sein, der nicht migriert wird. Weiter sollte bedacht werden, dass in der neuen Windows 2000-Infrastruktur Dateien und Registrierungseinträge aus der alten NT-Installation zu Problemen führen könnten.

Bei einer **Umstrukturierung** wird parallel zu der existierenden Windows NT-Umgebung zuerst eine neue, separate Windows 2000-basierte Infrastruktur aufgebaut. Danach werden die Objekte (z. B. Benutzer und Gruppen) aus dem bestehenden Windows NT-Domänenmodell in die neue Active Directory-Struktur übernommen. Dabei können einzelne oder auch mehrere Objekte gleichzeitig übertragen werden. Dieser Vorgang sollte konzeptionell gut geplant und die Reihenfolge der Objektmigration festgelegt werden. Durch den Aufbau einer zweiten Umgebung wird bei dieser Migrationsmethode wenig Einfluss auf das Produktionssystem genommen, allerdings erfordert sie zusätzlich den Einsatz eines Migrationsprogramms (siehe Tz. 3.1.2).

3.1.2 Active Directory-Migrationsprogramm

Das *Active Directory Migrations Tool (ADMT)* ist ein effektives Tool, das die Migration von Benutzern, Computern und Gruppen in neue Domänen vereinfacht.



Active Directory-Migrationsprogramm

Das *Active Directory Migrations Tool* bietet ein einfaches, sicheres und schnelles Verfahren für die

- Migration von Windows NT 4.0-Domänen auf Windows 2000-Domänen und die
- Neustrukturierung von bestehenden Windows 2000-Domänen.

Systemadministratoren können mögliche Probleme noch vor dem Beginn der Migrationsvorgänge diagnostizieren. Aufgabenbasierte Assistenten ermöglichen es auf einfache Weise, Benutzer, Gruppen und Computer zu verschieben, Dateiberechtigungen zu vergeben sowie Microsoft Exchange Server-Postfächer zu migrieren. Mit der **Berichtsfunktion** des Tools können die Auswirkungen der Migration vor und nach den Verschiebevorgängen bewertet werden.

Das Tool bietet auch Unterstützung für parallele Domänen. Es können die vorhandenen Domänen des Betriebssystems Microsoft Windows NT 4.0 beibehalten werden. Gleichzeitig ist *ADMT* so flexibel, dass jede Organisation einen seinen individuellen Bedürfnissen angepassten Migrationsvorgang implementieren kann.

Für die Migration können neben *ADMT* weitere Tools eingesetzt werden. Nachfolgend wird ihr Funktionsumfang gegenübergestellt.

Funktion	**ADMT**	**Clone Principal**	**MoveTree**	**NetDom**
Führt strukturübergreifende Kopieroperationen durch	×	×		×
Führt strukturinterne Verschiebeoperationen durch	×		×	×
Aktualisiert den SID-Verlauf, der Ressourcen verwendet	×	×	×	
Grafische Benutzeroberfläche	×			
Skriptgesteuerte Unterstützung		×	×	×
Behält Kennwörter bei	×		×	

Migriert Benutzer	×	×	×	
Migriert Gruppen	×	×	×	
Migriert Computer	×			×
Migriert Vertrauensstellungen	×			×
Migriert Organisationseinheiten			×	
Migriert Benutzerprofile	×			
Migriert Dienstkonten	×			
Aktualisiert Zugriffssteuerungslisten (ACLs) auf Ressourcen	×			
Synchronisiert Domänen				×

Das *Active Directory Migration Tool (ADMT)* erhalten Sie als kostenlosen Download (2,3 MB) auf der Webseite:
<www.microsoft.com/germany/ms/windows2000/upgrade/migration/admt.htm >

3.2 Migration auf Windows 2000 Professional/XP

Die Migration auf Windows 2000 Professional/XP ist in der Regel unproblematisch und nicht mit Änderungen der Domänenstruktur verbunden. Folgende frühere Versionen von Windows können aktualisiert werden:

Ursprung	**Aktualisierung auf**
Windows für Workgroups 3.1	Windows NT Workstation, danach Windows 2000 Professional bzw. XP
Windows 95 und Windows 98	Windows 2000 Professional bzw. XP
Windows NT Workstation 3.51 oder 4.0	Windows 2000 Professional bzw. XP

Bevor eine Aktualisierung durchgeführt wird, sollte mithilfe des *Windows 2000 Readiness Analyzer* ein Kompatibilitätsbericht erstellt werden (siehe Tz. 3.1).

Windows 2000/XP-Clients können auch an einen Windows NT 4.0-Domänencontroller angebunden werden. Die auf dem Server konfigurierten Clienteinstellungen (Profile, System- und Kennwortrichtlinien usw.) werden von dem Windows 2000-Client unterstützt.

3.3 Domänenkonzepte

Unter einer **Domäne** versteht man einen **logischen Verbund von Computern**, die eine gemeinsame **Benutzerkonten-Datenbank** verwenden und gemeinsame Sicherheitsrichtlinien benutzen. Benutzer, die auf eine Windows 2000 Server-Domäne zugreifen möchten, werden durch einen Domänencontroller authentifiziert. Die Anmeldung erfordert den Benutzernamen, das Kennwort und den Domänennamen. Innerhalb einer Domäne können auch weitere Windows-Server (Mitglieds- bzw. Anwendungsserver) existieren, die nicht als Domänencontroller eingerichtet sind.

Vorteile von Domänen:

Sicherheitsrichtlinien und -einstellungen (z. B. Administratorrechte und Zugriffssteuerungslisten) können nicht von einer Domäne auf eine andere übertragen werden.

Die Delegierung von Administratorrechten an Domänen oder Organisationseinheiten macht die Ernennung zahlreicher Administratoren mit weit reichenden Administratorrechten überflüssig.

Domänen unterstützen die Strukturierung des Netzwerkes, wodurch die jeweilige Aufbauorganisation besser nachgebildet werden kann.

Alle Domänencontroller in einer bestimmten Domäne sind in der Lage, Änderungen im Active Directory zu empfangen und diese Änderungen auf alle anderen Domänencontroller innerhalb der Domäne zu replizieren.

Eine einzelne Domäne kann sich über mehrere physische Standorte erstrecken. Durch die Verwendung einer Einzeldomäne lässt sich der Verwaltungsaufwand erheblich verringern.

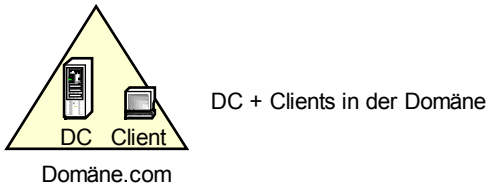
Zum Aufbau einer Domäne ist mindestens ein Computer erforderlich, auf dem eine der Server-Versionen von Windows 2000 ausgeführt wird und der als Domänencontroller konfiguriert ist. Jede Domäne sollte über wenigstens zwei Domänencontroller verfügen, um bei ei-

nem Ausfall des einen Domänencontrollers weiterhin die Anmeldung an der Domäne zu ermöglichen. Weiterhin kann bei dem Einsatz mehrerer Domänencontroller die durch das Bearbeiten der Anmeldungen entstehende Last auf mehrere Server verteilt werden.

Je nach administrativen Anforderungen und Netzwerkgröße gibt es verschiedene Möglichkeiten, eine Domäne anzulegen:

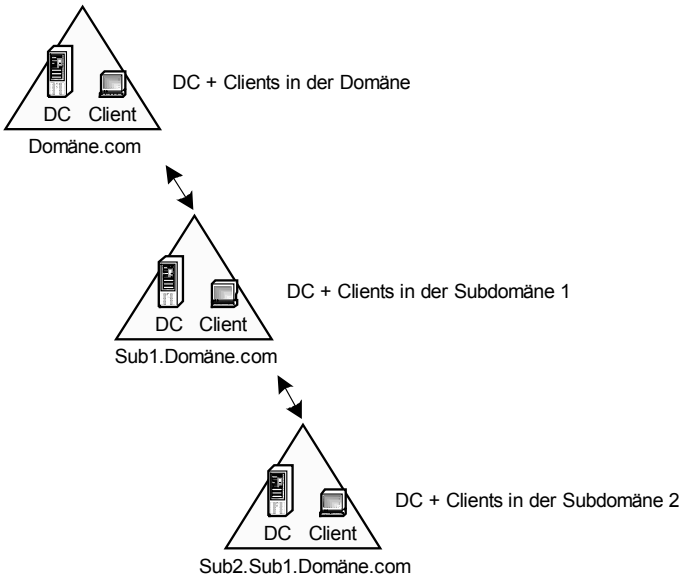
3.3.1 Einzeldomänenmodell (Single Domain Model)

Bei diesem Domänenkonzept werden alle Benutzer und Ressourcen in einer Domäne zusammengefasst. Dieses Modell bietet sich an, wenn die Zahl der Benutzer und das Netzwerk aus organisatorischen Gründen nicht aufgeteilt werden müssen.



Einzeldomänenmodell

3.3.2 Hauptdomänenmodell (Single Master Domain Model)

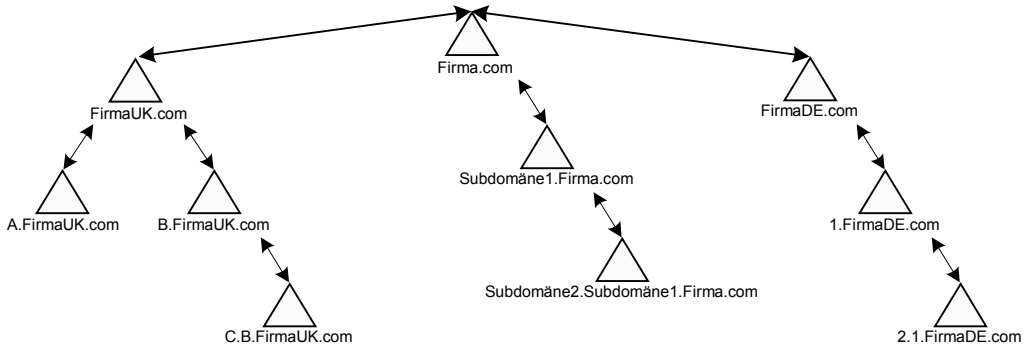


Hauptdomänenmodell

Dieses Domänenkonzept vereinigt die Vorteile der zentralen Benutzerkonten mit der Möglichkeit, das Netzwerk den organisatorischen Gegebenheiten entsprechend zu unterteilen. Es existiert eine **Master- bzw. Root-Domäne**, in der die Objekte der **gesamten** Domäne registriert werden (Schemamaster). Alle anderen Sub-Domänen im Netzwerk vertrauen der Root-Domäne und können somit auf die dort gespeicherten Informationen zugreifen.

3.3.3 Mehrfachhauptdomänenmodell (Multiple Master Domain Model)

Das Multiple Master Domain Model ist für sehr **große Netzwerke** geeignet. Neben einer Root-Domäne (z. B. Firma.com) gibt es weitere Master-Domänen, die sich gegenseitig vertrauen.



Mehrfachhauptdomänenmodell

Auch hier können z. B. die Benutzer- und Gruppenkonten von dezentralen Administratoren verwaltet werden. Da die Sub-Domänen ihrer Master-Domäne vertrauen, gelten die Einstellungen in der Domänengesamtstruktur (siehe Tz. 2.4.2).

3.4 Domänencontrollerfunktionen

Den Domänencontrollern stehen so genannte **Betriebsmasterfunktionen** zur Verfügung. Folgende Funktionen werden einem oder mehreren Domänencontrollern in einer Active Directory-Domäne zugewiesen:

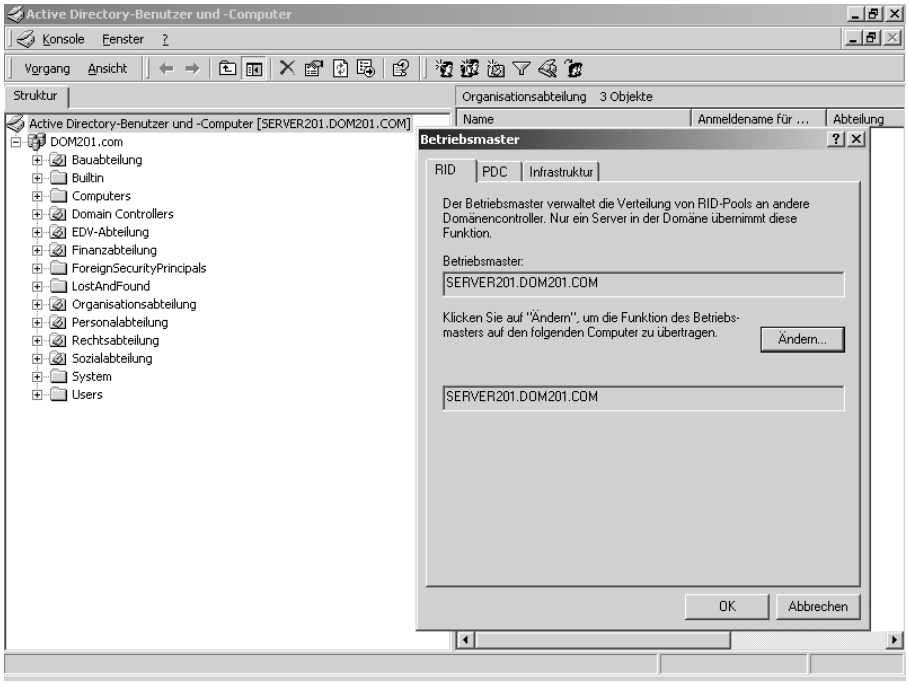
- Schemamaster (1 x je Domänengesamtstruktur),
- DNS-Master (1 x je Domänengesamtstruktur),
- RID-Master (1 x je Domäne),

- PDC-Emulator (1 x je Domäne),
- Infrastrukturmaster (1 x je Domäne).

Die Domänencontroller, denen diese Funktionen zugewiesen wurden, führen dann **Einzelmasteroperationen** aus.

Bestimmte Operationen dürfen nicht gleichzeitig an verschiedenen Standorten im Netzwerk vorgenommen werden. So muss z. B. die Erstellung von Sicherheits-IDs für Computer (Ressourcen) von einem einzelnen Domänencontroller durchgeführt werden, damit gewährleistet ist, dass eindeutige IDs vergeben werden (siehe grauer Kasten auf der nächsten Seite).

Dem **ersten** Domänencontroller in einer Domäne werden mit der Installation automatisch sämtliche Betriebsmasterfunktionen zugewiesen. Nach Abschluss der Installation kann die Zuweisung der Betriebsmasterfunktionen mit dem Verwaltungsprogramm *Active Directory-Benutzer und -Computer* geändert werden. Eine Änderung der Betriebsmasterfunktionen ist jedoch nur dann von Bedeutung, wenn sich Organisationen über mehrere Standorte erstrecken.



Betriebsmasterfunktionen im Active Directory-Benutzer und -Computer

Im Verwaltungsprogramm *Active Directory-Benutzer und -Computer* werden nur die Betriebsmasterfunktionen angezeigt, die einem Domänencontroller einer Domäne zugeordnet wurden. Sie können auf einen anderen Domänencontroller derselben Domäne übertragen werden.

Der *DNS-Master* kann hingegen mit dem Verwaltungsprogramm *Active Directory-Domänen und -Vertrauensstellungen* verwaltet werden. Um den *Schemamaster* zu administrieren, muss das Snap-In *Active Directory-Schema* über die Managementkonsole aufgerufen werden. Das setzt die Installation von *Adminpak* voraus (siehe Tz. 2.7).

Die Administration der Betriebsmasterfunktionen sollten Sie nur durchführen, wenn Sie die Zusammenhänge genau verstehen. Eine fehlerhafte Administration kann zu erheblichen Beeinträchtigungen bis hin zu einem Ausfall des entsprechenden Domänencontrollers führen.

Auf die Gesamtstruktur bezogene Betriebsmasterfunktionen

Jede Active Directory-Gesamtstruktur (eine oder mehrere Domänen) muss über folgende Funktionen verfügen:

- Schemamaster

  Das Schema beschreibt die **Objektklassen und Attribute**, die im Active Directory gespeichert sind. Im Schema sind für jede Objektklasse die erforderlichen Attribute, die möglichen zusätzlichen Attribute und die ihr übergeordnete Objektklasse definiert. Der Domänencontroller mit der Funktion des Schemamasters überwacht alle Aktualisierungen und Änderungen am Schema.

- Domänennamenmaster (DNS-Master)

  Der Domänencontroller mit der Funktion des DNS (Domain Name System)-Masters steuert das **Hinzufügen oder das Entfernen** von Domänen in der Gesamtstruktur, um Namenskonflikte zu vermeiden.

Diese beiden Funktionen dürfen **nur einmal innerhalb der Domänengesamtstruktur** vorhanden sein. In der Regel verfügt der erste Domänencontroller über diese Funktionen.

Domänenweite Betriebsmasterfunktionen

Jede Domäne in der Gesamtstruktur muss über folgende Funktionen verfügen:

- RID (Relative ID)-Master

  Jedes auf einem Domänencontroller erstellte Objekt erhält eine domänenweite **Sicherheitskennung** (Security-ID, SID). Im Active Directory ist diese Security-ID eine Kombination der Domänensicherheitskennung plus einer domänenweiten eindeutigen relativen Kennung (RID). Der RID-Master erstellt den **zweiten Teil** dieser Security-ID und ist für die Zuweisung dieses RID-Pools zuständig.

Jeder Domänencontroller bekommt einen **RID-Pool** vom RID-Master zur Verfügung gestellt. Wenn auf einem Domänencontroller z. B. ein Benutzer oder eine Gruppe angelegt wird, weist er dem entsprechenden Objekt eine eindeutige Security-ID (SID = Domänenkennung + RID) zu, indem er eine RID aus dem ihm zugewiesenen RID-Pool benutzt.

- PDC-Emulation (Primary Domain Controller)

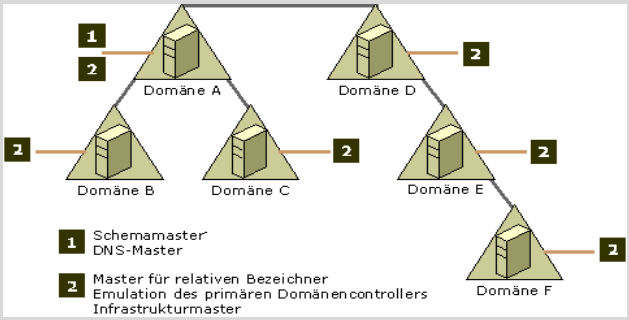
  Der PDC-Betriebsmaster hat im **gemischten Modus** u. a. die Aufgabe, als PDC für Windows NT-Backupdomänencontroller zu fungieren, wenn mit Domänen gearbeitet wird.

  In einer Windows 2000-Domäne im **einheitlichen Modus** empfängt die PDC-Emulation die Replikation von Kennwortänderungen, die von anderen Domänencontrollern in der Domäne ausgeführt werden. Wurde ein Kennwort kürzlich geändert, dauert es einige Zeit, bis diese Änderung auf alle Domänencontroller in der Domäne repliziert wurde. Kann die Anmeldung aufgrund eines ungültigen Kennwortes auf einem anderen Domänencontroller nicht authentifiziert werden, leitet dieser Domänencontroller die Authentifizierungsanforderung an die PDC-Emulation weiter, bevor der Anmeldeversuch zurückgewiesen wird.

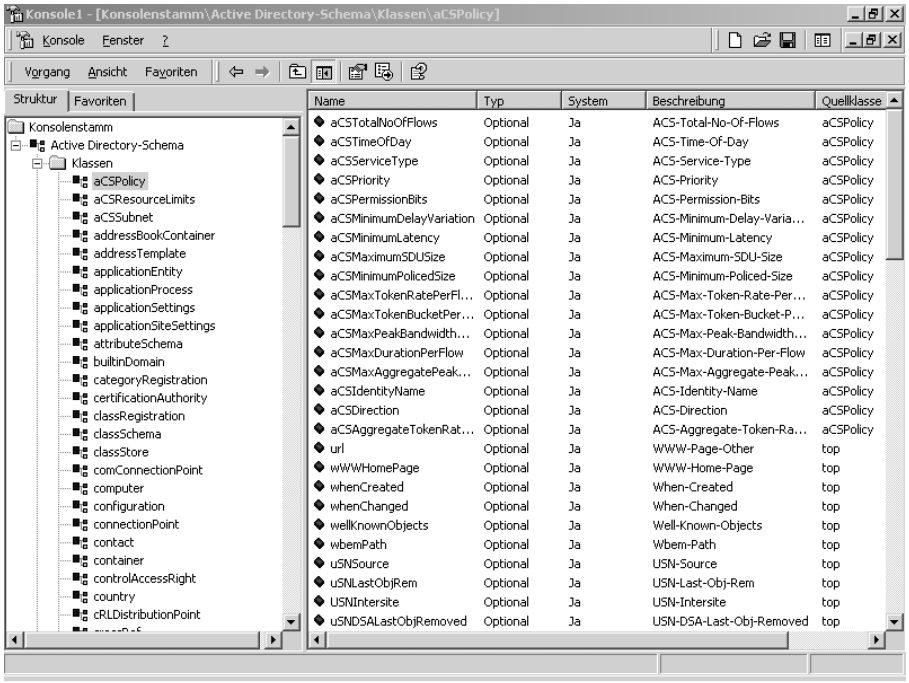
- Infrastrukturmaster

  Der Infrastrukturmaster verwaltet die Zuordnung von Benutzern zu Gruppen, wenn die Mitglieder einer Gruppe umbenannt oder geändert werden. Wenn z. B. ein Benutzer einer Gruppe verschoben wird und dieser Benutzer aus einer anderen Domäne stammt als die Gruppe, dann ist der Infrastrukturmaster für die Änderung der Gruppeninformationen verantwortlich, sodass der neue Standort des Benutzers gefunden wird. Die vom Infrastrukturmaster ausgeführte Aktualisierung wird mittels Replikation auf andere Domänencontroller verteilt. Jeder Infrastrukturmaster bearbeitet nur die Konten der eigenen Domäne.

Diese Funktionen dürfen nur **einmal in jeder Domäne** vorhanden sein. Das bedeutet, dass es in jeder Domäne der Gesamtstruktur nur einen RID-Master, eine PDC-Emulation und einen Infrastrukturmaster geben darf.



Struktur der Betriebsmasterfunktionen



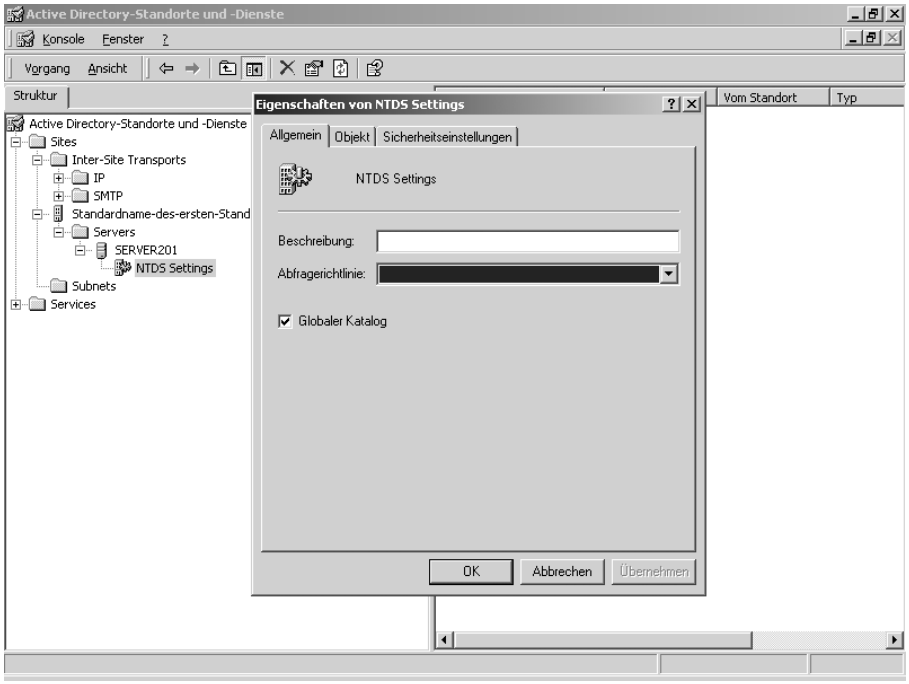
Active Directory-Schema

Neben den Betriebsmasterfunktionen verfügt Windows 2000 über einen so genannten *Globalen Katalog*. Der *Globale Katalog* erfüllt zwei wichtige Aufgaben:

- Er erlaubt ein schnelles Finden der Ressourcen in einer Domänengesamtstruktur.
- Er liefert dem Domänencontroller Informationen über die Gruppenmitgliedschaften und nimmt die Benutzeranmeldung entgegen.

Der *Globale Katalog* ist neben dem Active Directory als eine zusätzliche Datenbank zu verstehen. In dieser Datenbank wird eine Untermenge der Objektattribute von allen Objekten der Domänengesamtstruktur gespeichert. Der *Globale Katalog* enthält z. B. Objektattribute über den Anmeldenamen, Familiennamen, Vornamen, E-Mail-Adressen von Benutzern. Darüber hinaus wird auch der Ort (Lokation) des Objektes gespeichert.

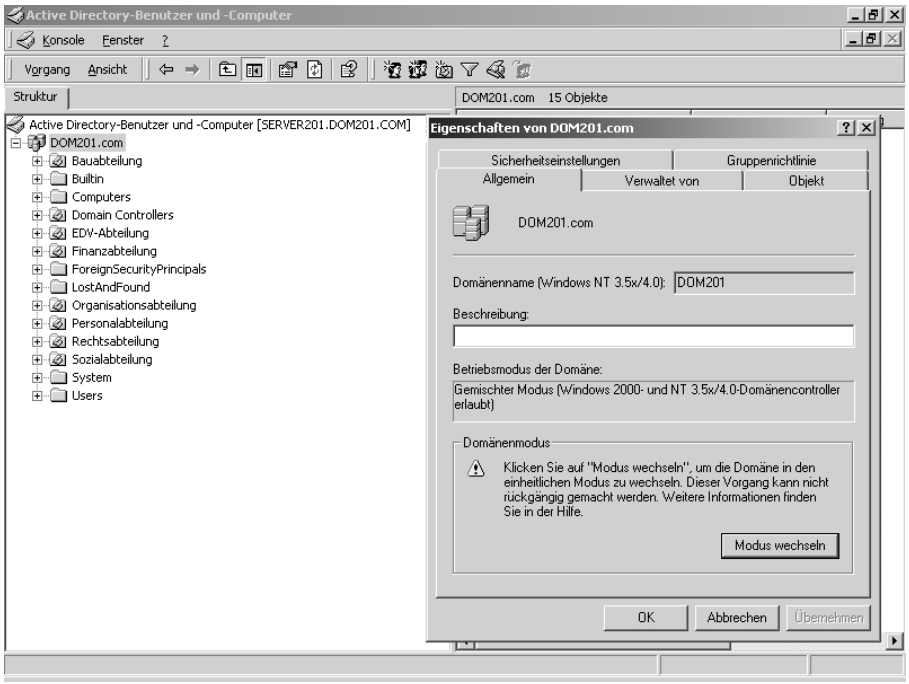
Der **erste** Domänencontroller in einer Domänengesamtstruktur verfügt immer über einen *Globalen Katalog*. Je nach Größe der Domänengesamtstruktur können auf weiteren Domänencontrollern ein *Globaler Katalog* eingerichtet werden, um z. B. den Netzwerkverkehr durch Ressourcensuche zu minimieren.



Active Directory-Standorte und -Dienste – Eigenschaften von NTDS-Settings

3.5 Domänenmodus

Aufgrund der Verwendung unterschiedlicher Gruppenkonten in Windows 2000 und Windows NT können zwei Domänenmodi verwendet werden.



Active Directory-Benutzer und -Computer, Betriebsmodus

Im **gemischten Modus** können Windows 2000-Domänencontroller und Windows NT-Backupdomänencontroller (BDC) in einer Domäne vorhanden sein. Im gemischten Modus werden weder universelle noch verschachtelte Gruppenerweiterungen von Windows 2000 unterstützt. Der gemischte Modus ist nach der Installation von Windows 2000 standardmäßig eingestellt.

Die Einstellungen für den Domänenmodus können in Windows 2000 zum **einheitlichen Modus** geändert werden. Dieser Zustand tritt ein, wenn alle Domänencontroller der Domäne auf Windows 2000 umgestellt wurden und ein Administrator den einheitlichen Modus aktiviert hat.

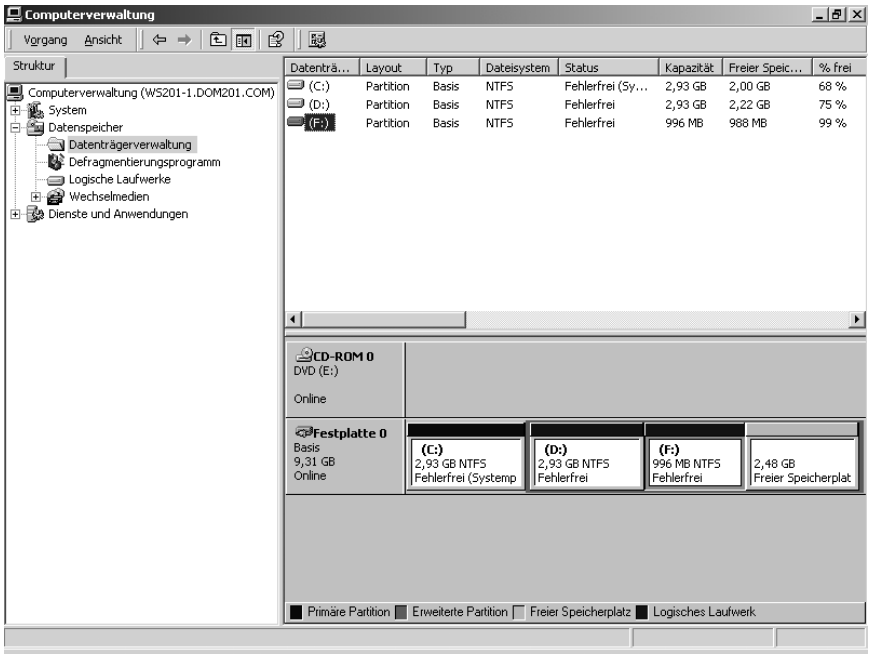
Einen Wechsel vom gemischten Modus in den einheitlichen Modus können Sie **nicht** rückgängig machen. Insofern ist vor der Umstellung sicherzustellen, dass die Windows NT-Backupdomänencontroller (BDC) aktualisiert oder durch Windows 2000-Domänencontroller ersetzt wurden.

3.6 Datenträger und Dateisysteme

3.6.1 Datenträger

Die Datenträgerverwaltung (Snap-In) im Programm *Computerverwaltung* ist ein Systemprogramm zur Verwaltung von Festplatten und den auf ihnen enthaltenen Partitionen. Vor der Installation von Windows 2000 ist zu berücksichtigen, wie die Festplatte des Systems einzurichten ist. Mit der Datenträgerverwaltung können Datenträger formatiert und Dateisysteme erstellt werden. Über das Netzwerk kann der Administrator von jedem Windows 2000-Computer die Datenträger (Festplatten) anderer Windows 2000-Computer verwalten.

Die Datenträgerverwaltung unterstützt **Basisfestplatten** und **dynamische Festplatten**. Basisfestplatten verwenden das partitionsorientierte Schema der Festplattenstrukturierung, das auch Windows NT Server 4.0 nutzt. Dynamische Festplatten hingegen werden nicht mehr als Partitionen, sondern als *Datenträger* (Definition im grauen Kasten, auf der nächsten Seite) eingerichtet. Die Bearbeitung des *Datenträgers* kann im laufenden Betrieb vorgenommen werden.



Datenträgerverwaltung – Clientzugriff über das Netzwerk (Basisfestplatte)

Standardmäßig wird bei der Installation von Windows 2000 die Festplatte als Basisfestplatte eingerichtet. Bei der Umstellung von Windows NT 4.0 auf Windows 2000 werden partitionierte Festplatten automatisch als Basisfestplatten initialisiert, sodass die mit Windows NT Server 4.0 erstellten Partitionen beibehalten werden können. Neue und unbeschriebene Festplatten können nach der Installation als Basisfestplatten oder als dynamische Festplatten eingerichtet werden.

Datenträger auf dynamischen Festplatten

Einfacher Datenträger

Ein *Einfacher Datenträger* kann nur auf einer **dynamischen Festplatte** erstellt werden. Er entspricht einer primären Partition einer Basisfestplatte. Der Datenträger kann aus einem einzelnen oder aus mehreren miteinander verknüpften Bereichen auf einer Festplatte bestehen. Ein *Einfacher Datenträger* kann auf derselben Festplatte oder über zusätzliche Festplatten erweitert werden. Wird er über mehrere Festplatten erweitert, entsteht ein *Übergreifender Datenträger*.

Übergreifender Datenträger

Ein *Übergreifender Datenträger* umfasst einen Speicherplatz, der sich auf **mehreren physischen Festplatten** befindet. Es besteht die Möglichkeit, jederzeit den Speicherplatz zu erweitern. Ein *Übergreifender Datenträger* kann nicht gespiegelt werden.

Stripeset-Datenträger

Ein *Stripeset-Datenträger* speichert Daten in *Stripes* auf **zwei oder mehr physischen Fest-**

platten. Daten auf einem *Stripeset-Datenträger* werden abwechselnd und gleichmäßig (in Stripes) auf den verfügbaren Festplatten gespeichert. *Stripeset-Datenträger* verfügen über die besten Leistungsparameter unter Windows 2000. Wenn eine der Festplatten in einem *Stripeset-Datenträger* versagt, gehen die Daten auf dem **gesamten** Datenträger verloren.

Gespiegelter Datenträger

Bei einem *Gespiegelten Datenträger* handelt es sich um einen fehlertoleranten Datenträger, der Daten auf **zwei physische Datenträger** dupliziert. Hierbei entsteht eine **Datenredundanz**, indem die auf dem Datenträger enthaltenen Informationen unter Verwendung einer Kopie (Spiegel) des Datenträgers dupliziert werden. Der Spiegel befindet sich immer auf einem anderen Datenträger. Wenn einer der physischen Datenträger versagt, gehen die Daten auf dem beschädigten Datenträger verloren. Das System arbeitet jedoch weiter, da es auf den unbeschädigten Datenträger zurückgreifen kann. Leseoperationen werden auf einem *Gespiegelten Datenträger* langsamer ausgeführt als auf einem RAID-5-Datenträger, Schreiboperationen dagegen schneller.

RAID-5-Datenträger

Ein *RAID-5-Datenträger* ist ein fehlertoleranter Datenträger mit Daten und **Paritäten**, die über **drei oder mehr physische Festplatten** verteilt sind. Die Parität ist ein berechneter Wert, der nach Auftreten eines Fehlers zur **Datenrekonstruktion** verwendet wird. Wenn ein Teil einer physischen Festplatte ausfällt, können die Daten aus diesem fehlerhaften Bereich aus den verbleibenden Daten und der Parität wiederhergestellt werden. *RAID-5-Datenträger* können weder erweitert noch gespiegelt werden.

Die folgenden Funktionen stehen für Basisfestplatten und dynamische Festplatten zur Verfügung:

- Überprüfung der Datenträgereigenschaften, z. B. den Gesamtspeicherplatz, den freien Speicherplatz und den aktuellen Status,
- Anzeigen der Datenträger- und Partitionseigenschaften, wie z. B. Speicherkapazität, Laufwerkbuchstabenzuordnung, Bezeichnung, Typ und Dateisystem,
- Zuordnung von Laufwerkbuchstaben zu Festplattendatenträgern oder Partitionen und zu CD-ROM-Geräten,
- Einrichten von Festplattenfreigaben und Sicherheitsmaßnahmen für einen Datenträger bzw. eine Partition und
- Umwandlung einer Basisfestplatte in eine dynamische Festplatte und umgekehrt.

Für die Verwaltung von dynamischen Festplatten stehen zusätzliche Funktionen zur Verfügung:

- Erstellen und Löschen von *Einfachen*, *Übergreifenden*, *Stripeset-*, *Gespiegelten* und *RAID-5-Datenträgern*,
- Erweiterung eines *Einfachen* oder *Übergreifenden Datenträgers*,
- Entfernen der Spiegelung von einem *Gespiegelten Datenträger* und Aufteilen eines Datenträgers in zwei Datenträger und
- Reparatur von *Gespiegelten* und *RAID-5-Datenträgern*.

- Vor der Konvertierung sollten Sie ein nicht zugeordneten Speicherplatz von mindestens 1 MB auf der Festplatte berücksichtigen. In diesem Bereich wird nach dem Konvertierungsvorgang eine Datenbank mit den Konfigurationseinstellungen der Datenträger gespeichert.
- Ist auf einer Basisfestplatte bereits eine Partition eingerichtet, können Sie diese Partition bei einer Umwandlung in eine dynamische Festplatte nicht erweitern. Es lassen sich nur Partitionen erweitern, die nach der Einrichtung einer dynamischen Festplatte angelegt werden (siehe Laufwerk G: der Abbildung: Datenträgerverwaltung – Clientzugriff über das Netzwerk).
- Befindet sich auf einer Basisfestplatte eine FAT-Partition, wird diese bei der Umwandlung in eine dynamische Festplatte automatisch in eine NTFS-Partition konvertiert.
- Die Option zum Konvertieren einer Festplatte in eine dynamische Festplatte steht Ihnen auf einem tragbaren Computer nicht zur Verfügung. Dynamische Festplatten werden auf tragbaren Computern nicht unterstützt.

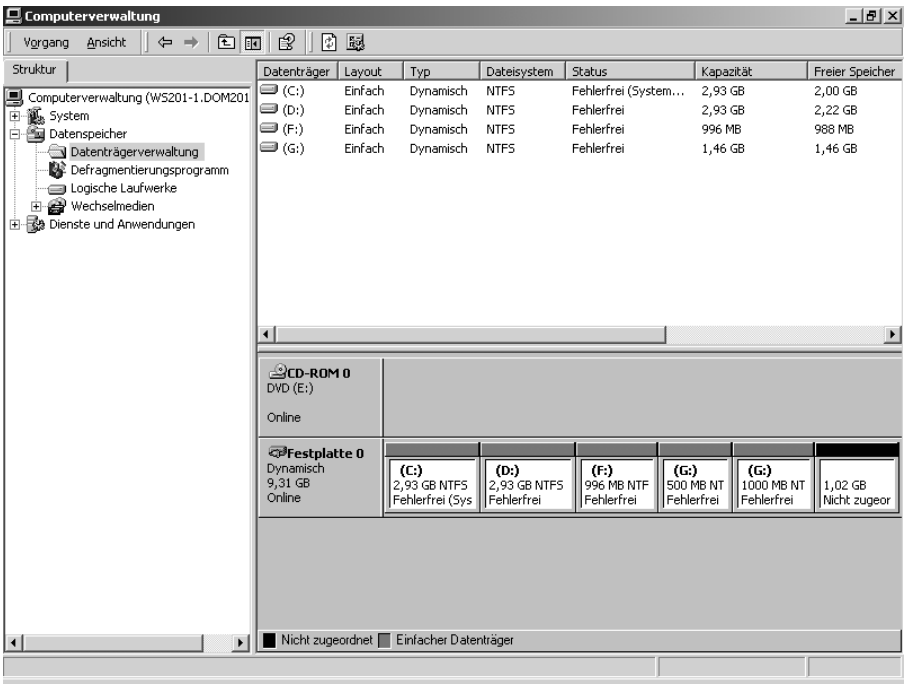
Dynamische Festplatten sind einzurichten, um ein **fehlertolerantes Festplattensystem** zu erstellen und Änderungen bzw. **Kapazitätserweiterungen** an Festplatten im laufenden Betrieb durchführen zu können.

Basisfestplatte in dynamische Festplatte umwandeln!

1. *Starten Sie die Computerverwaltung und klicken Sie auf Datenträgerverwaltung.*
2. *Klicken Sie mit der rechten Maustaste im unteren Fensterausschnitt auf die Festplatte, die zu einer dynamischen Festplatte konvertiert werden soll.*
3. *Klicken Sie auf IN DYNAMISCHE FESTPLATTE UMWANDELN und folgen Sie den Systemaufforderungen.*

Dynamische Festplatten können von anderen Betriebssystemen wie beispielsweise MS-DOS, Windows 9x und Windows NT nicht erkannt und genutzt werden.

Das Umwandeln einer Basisfestplatte in eine dynamische Festplatte lässt sich nur bedingt rückgängig machen. Während sich eine Basisfestplatte mit vorhandenen Daten in eine dynamische Festplatte umwandeln lässt, gilt dies nicht für die Rückumwandlung einer dynamischen Festplatte in eine Basisfestplatte. Es müssen zunächst die eingerichteten Datenträger entfernt werden.



Datenträgerverwaltung – Clientzugriff über das Netzwerk (Dynamische Festplatte)

Die o. a. Abbildung veranschaulicht folgende Strukturen der Datenträgerverwaltung:

- Die Festplatte ist in eine dynamische Festplatte umgewandelt worden.
- Es sind einfache Datenträger (Laufwerke D:, F: und G:) erstellt worden.
- Die Kapazität des Datenträgers G: wurde erhöht.
- Es ist noch ca. 1 GB freier Speicherplatz zur Erweiterung eines vorhandenen Datenträgers oder zur Einrichtung eines neuen Datenträgers als Laufwerk H: verfügbar.
- Die Rückumwandlung in eine Basisfestplatte ist nicht möglich, da auf dem Datenträger C:\ bereits das Betriebssystem installiert ist.

3.6.2 Dateisysteme

Weiterhin ist bei der Einrichtung eines Datenträgers festzulegen, welches **Dateisystem** verwendet werden soll. Windows 2000 unterstützt folgende Dateisysteme:

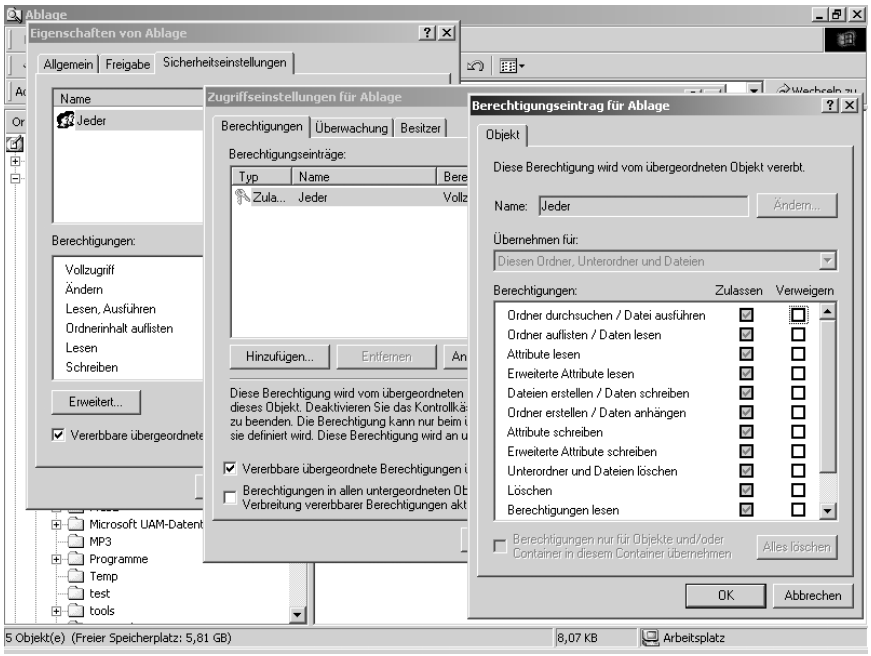
- NTFS (New Technology File System)

  NTFS (Version 5) bietet alle grundlegenden Funktionen der FAT-Dateisysteme. Jedoch ist NTFS sehr viel leistungsfähiger und verfügt über eine höhere Dateisicherheit, eine stärkere Datenträgerkomprimierung und unterstützt große Festplatten bis zu 2 TB (Terabyte). Gegenüber Windows NT 4.0 können zusätzliche Funktionen, wie Datenträgerkontingente und EFS (Encrypting File System), genutzt werden. Auf NTFS-Partitionen können den Benutzern und Gruppen weiter gehende Zugriffsrechte erteilt werden (siehe Abbildung nächste Seite).

- FAT bzw. FAT32 (File Allocation Table)

  FAT ist das Dateisystem von Windows 95 bzw. 98. FAT32 unterstützt Partitionen, die größer als 2 GB sein können. Somit müssen Festplatten nicht mehr in mehrere Partitionen unterteilt werden. FAT und FAT32 unterstützen jedoch nicht die Vergabe von Zugriffsberechtigungen auf Dateien und Ordner. Sie sind deshalb für eine ordnungsgemäße Datenverwaltung bzw. Datenabschottung ungeeignet.

Verwenden Sie bei der Installation von Windows 2000 nicht das Dateisystem FAT bzw. FAT32. Formatieren Sie die Festplatte ausschließlich mit dem Dateisystem NTFS, um die Vergabe von Zugriffsberechtigungen auf Dateien und Ordner zu ermöglichen. Eine unter FAT oder FAT32 eingerichtete Festplatte kann nachträglich über die *Eingabeaufforderung* mit dem Befehl `convert` nach NTFS konvertiert werden. Sichern Sie jedoch vor dem Konvertieren Ihre Daten.



Berechtigungen auf den Ordner „Ablage“

3.7 Sicherheitscheck

- *Führen Sie die **Migration** von Windows NT 4.0 auf Windows 2000 Server **parallel** zum bestehenden Windows NT-Umfeld durch.*
- *Setzen Sie für die Migration der Domänencontroller das **Active Directory Migrations Tool (ADMT)** ein.*
- *Legen Sie in Abhängigkeit von der Größe der Organisation das passende **Domänenkonzept** fest.*
- *Führen Sie nur Änderungen der **Betriebsmasterfunktionen** durch, wenn mehrere Domänencontroller eingesetzt werden. Planen Sie die Änderung sorgfältig.*
- *Führen Sie den Wechsel vom gemischten in den einheitlichen Modus erst nach erfolgreichem **Abschluss** der Migration durch.*

- *Richten Sie Gespiegelte oder RAID-5-Datenträger ein, um eine hohe **Verfügbarkeit** auf Datenbestände der Server zu gewährleisten.*
- *Formatieren Sie die Datenträger auf den Festplatten mit dem **Dateisystem NTFS**.*

4 Domain Name System (DNS)

In diesem Kapitel erfahren Sie,

- welche Bedeutung Domain Name System (DNS) unter Windows 2000 hat,
- warum DNS die Voraussetzung für den Einsatz des Active Directory ist,
- wie Host- bzw. Computernamen in IP-Adressen umgewandelt werden,
- was unter einer Zone und dem Zonentyp zu verstehen ist,
- wie DNS installiert und konfiguriert wird und
- welches Programm für einen Funktionstest von DNS eingesetzt werden kann.

4.1 Bedeutung des Domain Name System (DNS)

Beim Domain Name System (DNS) handelt es sich um eine verteilte Datenbank, die in TCP/IP-Netzwerken zur Übersetzung von Computernamen (Hostnamen) in IP-Adressen eingesetzt wird. Die Auflösung von Hostnamen mithilfe von DNS bietet folgende Vorteile:

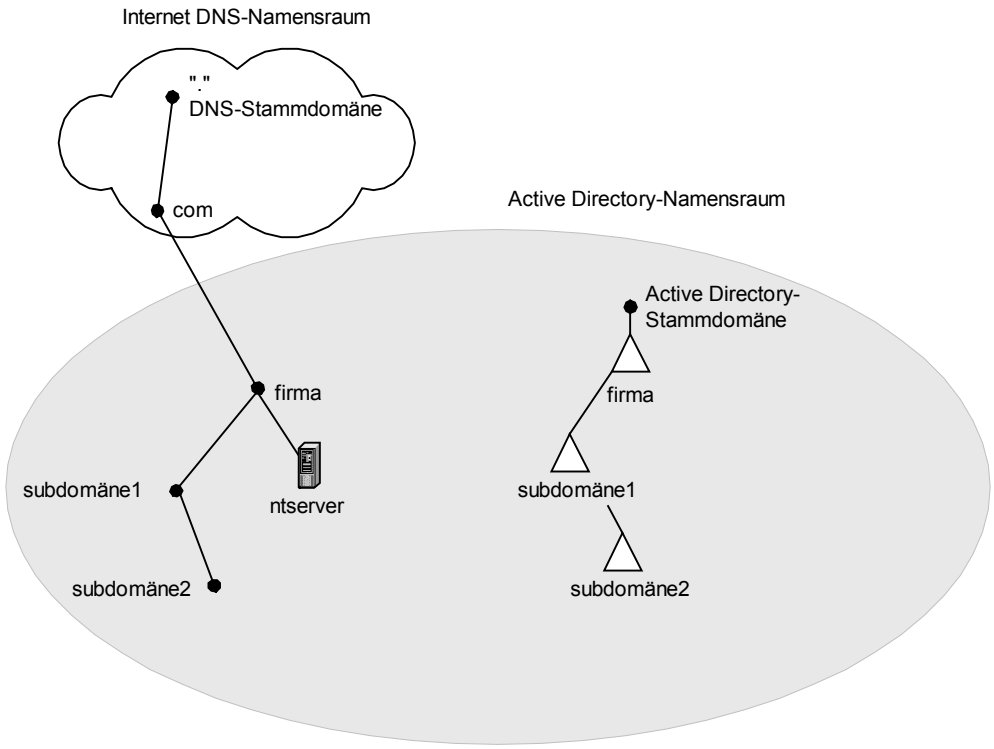
- Hostnamen sind benutzerfreundlich, da sie leichter zu merken sind als IP-Adressen.
- Hostnamen sind konstanter als IP-Adressen. Die IP-Adresse eines Servers kann sich ändern, sein Name bleibt jedoch gleich.
- Hostnamen ermöglichen den Benutzern unter Verwendung der gleichen Benennungskonventionen wie im Internet eine Verbindung zu lokalen Servern herzustellen.

DNS-Namen setzen sich folgendermaßen zusammen:

- **FQDN (Full Qualified Domain Name):** Das ist der vollständige, qualifizierte Name, der sich aus Hostname und einem der zur Verfügung stehenden Suffixe zusammensetzt, z. B. host1.firma.com.
- **Hostname:** Dieser Name bezeichnet einen Computer innerhalb einer Domäne. Im lokalen Netz reicht der Name zur vollständigen Beschreibung aus, z. B. host1.

- **Primäres DNS-Suffix:** Dieses Suffix (Erweiterung, Zusatzkennzeichen) wird an den Hostnamen angehängt, um den FQDN zu erhalten, z. B. firma.com.

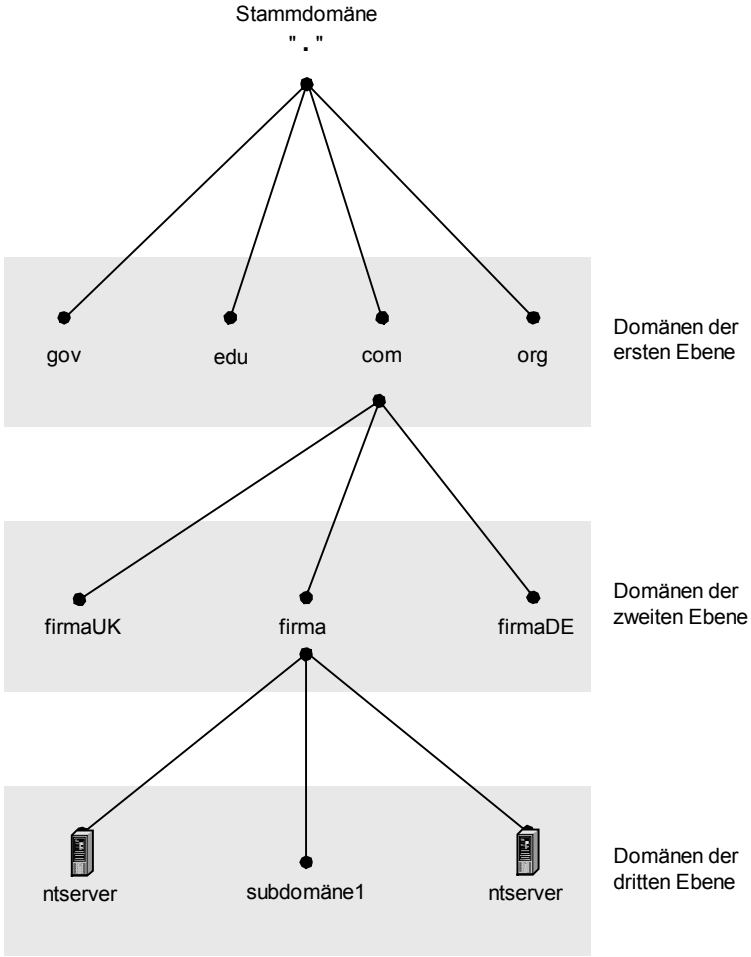
Verbindungsspezifisches Suffix: Dieses Suffix ist an den Netzwerkadapter gebunden, über den eine Verbindung hergestellt wird. Damit können unterschiedliche Namen im lokalen Netz und im Internet verwendet werden.



DNS-Namensraum im Internet und im Active Directory

- Der Begriff **Domäne** (bzw. Domain) hat im Zusammenhang mit DNS eine andere Bedeutung als der Begriff Domäne im Zusammenhang mit Windows 2000 Active Directory.
- Eine **Windows 2000-Domäne** stellt eine Struktur dar, die durch den Inhalt des Active Directory-Informationsspeichers begrenzt wird.
- Eine **DNS-Domäne** ist ein Namensraum (Namespace), der begrenzt wird durch den Inhalt der DNS-Datenbank, die als Zonendatei bezeichnet wird.
- Bei Windows 2000 haben beide Domänenstrukturen im Active Directory eine gemeinsame Schnittstelle, denn Active Directory ist auf DNS angewiesen, um seinen Namensraum zu definieren.

Der DNS-Name (FQDN) ist streng hierarchisch aufgebaut und wird von hinten nach vorne gelesen. Die **Stammdomäne** (Wurzel, Root) ist die oberste Domäne einer Hierarchie und verwendet eine Nullbezeichnung.



DNS-Namenshierarchie

Direkt unterhalb der Stammdomäne befinden sich die Domänen der ersten Ebene (Top-Level-Domänen). Sie werden nach **Organisationstyp** (Namenscode mit 3 Zeichen) oder der **geographischen Lage** (Namenscode mit 2 Zeichen) eingeteilt.

Auf der nächsten Ebene innerhalb des hierarchischen DNS-Namensraums befinden sich die Domänen der zweiten Ebene (Second-Level-Domänen). Sie können sowohl **Hosts** als auch **Teildomänen** (z. B. firma.com) enthalten.

Unterhalb einer Domäne der zweiten Ebene liegen die Domänen der dritten, vierten usw. Ebene. Die Domäne firma.com kann beispielsweise Computer (z. B. ntserver.firma.com) sowie Teildomänen (z. B. subdomäne1.firma.com) beinhalten. Die Teildomäne subdomäne1.firma.com kann wiederum Hosts oder weitere Teildomänen enthalten.

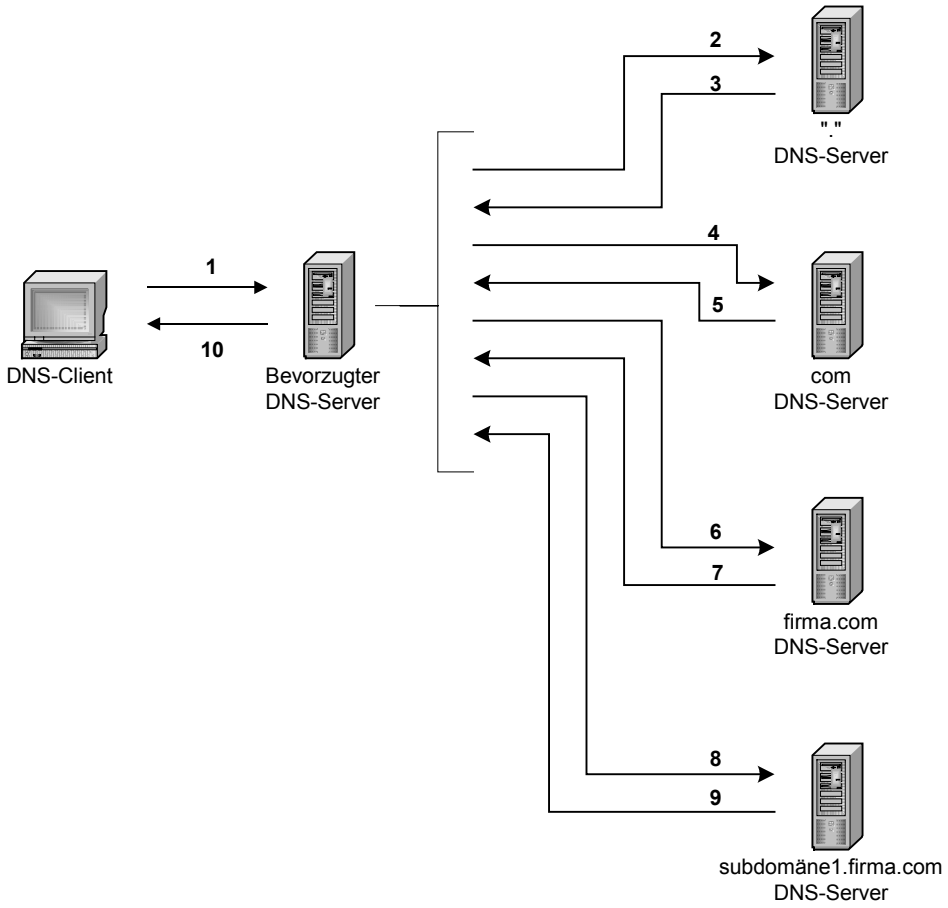
Domänen der ersten Ebene	Beschreibung
com	commercial = Kommerzielle Organisationen
org	organization = Nicht kommerzielle Organisationen
net	network = Internet-Service-Provider
edu	educational = Bildungseinrichtungen
gov	government = Regierungen
mil	military = Militärische Einrichtungen
int	international = Internationale Einrichtungen
de	Ländercode Deutschland
us	Ländercode Vereinigte Staaten von Amerika

4.2 Überblick über den Vorgang der Namensauflösung

Die Namensauflösung ähnelt dem Nachschlagen eines Namens im Telefonbuch. Jeder Name ist mit einer Telefonnummer bzw. mit einer IP-Adresse verknüpft. Wenn beispielsweise durch Eingabe der Webseite www.firma.de eine Verbindung zu dieser Webseite hergestellt wird, löst DNS diesen Namen in die zugehörige IP-Adresse auf. Die Zuordnung von Namen und IP-Adressen wird in der verteilten DNS-Datenbank gespeichert.

DNS-Namenserver können Abfragen für beide Richtungen einer Namensauflösung verarbeiten. Bei einem ***Forward-Lookup*** wird ein Name in eine IP-Adresse aufgelöst. Bei einem ***Reverse-Lookup*** wird hingegen eine IP-Adresse in einen Namen übersetzt. Ein DNS-Namenserver kann nur Abfragen zur Namensauflösung für eine **Zone** durchführen, für die dieser Autorität besitzt. Kann er eine Abfrage zur Namensauflösung nicht bearbeiten, wird die Anforderung an denjenigen DNS-Namensserver übergeben, der die Anforderung bearbeiten kann.

Im nachfolgenden Beispiel möchte der DNS-Client den Namen **host1.subdomäne1.firma.com** auflösen:



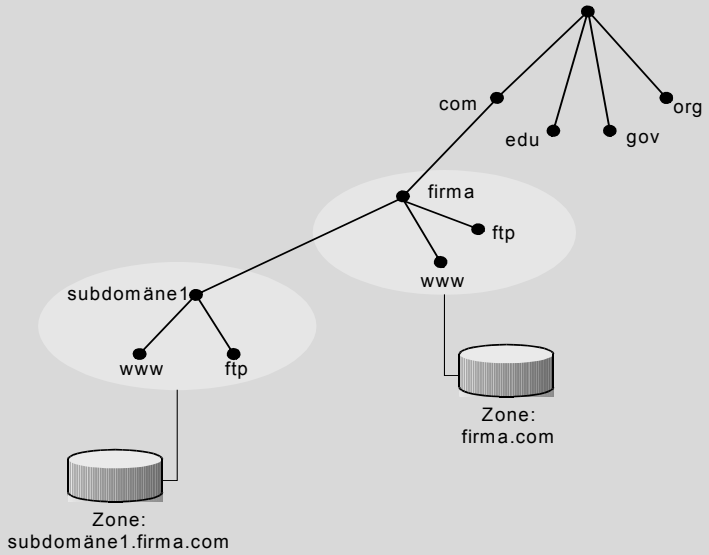
DNS-Namensauflösung

In seinem lokalen Speicher vorheriger DNS-Abfragen findet er keinen Eintrag zu diesem Namen, deshalb schickt er eine Abfrage an den bevorzugten DNS-Namensserver (1). Dieser versucht zunächst, den Namen über die lokalen Zonendaten (siehe grauer Kasten) oder die im Cache zwischengespeicherten Einträge aufzulösen. Findet er einen Eintrag, der mit dem gesuchten Namen übereinstimmt, antwortet er dem DNS-Client, indem er den Namen auflöst. Der Abfragevorgang wäre in diesem Fall abgeschlossen. Kann der Name auf diesem Weg jedoch nicht aufgelöst werden, werden weitere evtl. vorhandene DNS-Namensserver abgefragt. Es wird somit ein so genannter *Rekursivprozess* in Gang gesetzt (2 - 9). Der bevorzugte DNS-Namensserver schickt nach Analyse des Namens beispielsweise

- eine Abfrage zum DNS-Stamm-Namensserver, der mit einem Verweis auf den DNS-Namensserver "com" antwortet (2/3),
- eine Abfrage zum DNS-Namensserver "com", der mit einem Verweis auf den DNS-Namensserver "firma" antwortet (4/5),
- eine Abfrage zum DNS-Namensserver "firma", der mit einem Verweis auf den DNS-Namensserver "subdomäne1" antwortet (6/7) und
- eine Abfrage zum DNS-Namensserver "subdomäne1", der die **Adresse** von host1.subdomäne1.firma.com zurückgibt (8/9).
- Der bevorzugte DNS-Namensserver gibt die Informationen an den ursprünglich anfragenden DNS-Client zurück (10) und schließt damit den Rekursiv-Abfrageprozess ab. Er speichert die Abfrageergebnisse für einen bestimmten Zeitraum im Cache, um den Datenverkehr im Netzwerk zu reduzieren. Dieser Zeitraum wird als TTL (Time To Live) bezeichnet. Die Zone, die das Abfrageergebnis bereitstellt, legt auch die TTL fest. Die TTL kann über die Zoneneigenschaften in der DNS-Managementkonsole konfiguriert werden.

Zone

In einer Zone werden Internetnamen definiert, die in einer bestimmten Zonendatei (z. B. firma.com.dns) verwaltet werden. Eine größere Domäne kann in mehrere Zonen aufgeteilt werden, um z. B. Verwaltungsaufgaben voneinander abzugrenzen. Ein DNS-Server kann eine oder mehrere Zonen verwalten.



Zonenaufteilung einer Domänengesamtstruktur

Zonenname

Üblicherweise wird eine Zone nach der höchsten Domäne in der Hierarchie benannt, der die Zone angehört (siehe Abbildung).

Zonendatei

Die Zonendatei beinhaltet alle Daten für die Namensauflösung. Standardmäßig wird der Zonenname mit der Erweiterung .dns versehen. Wenn der Zonenname beispielsweise firma.com lautet, wird als Standardname für die Zonendatenbankdatei der Name *firma.com.dns* verwendet. Die Datei wird im Verzeichnis Stammverzeichnis:\System32\DNS gespeichert.

Zonentyp

Es kann zwischen primären, sekundären und Active Directory-integrierten Zonen unterschieden werden:

Primär: In einer primären Zone wird die Original-Zonendatei von einem primären DNS-Server verwaltet. Die DNS-Daten sind in einer Standardtextdatei lokal im Verzeichnis c:\winnt\system32\dns gespeichert. Diese Option erleichtert den Austausch von DNS-Daten mit anderen DNS-Servern, die textbasierte Speichermethoden einsetzen.

Sekundär: In einer sekundären Zone kopiert ein sekundärer DNS-Server die Zonendatei eines anderen Servers, der wiederum primär oder sekundär sein kann. Eine sekundäre Zone kann erstellt werden, um eine Redundanz zu gewährleisten und die Last der Namensauflösung zu verteilen.

Active Directory-integriert: In einer Active Directory-integrierten Zone wird die Zonendatei im Active Directory gespeichert. Bei der Active Directory-Verzeichnisreplikation werden nur die relevanten Änderungen übermittelt. Daher ist sie schneller und effizienter als die Standard-DNS-Replikation.

4.3 Installation und Konfiguration von DNS

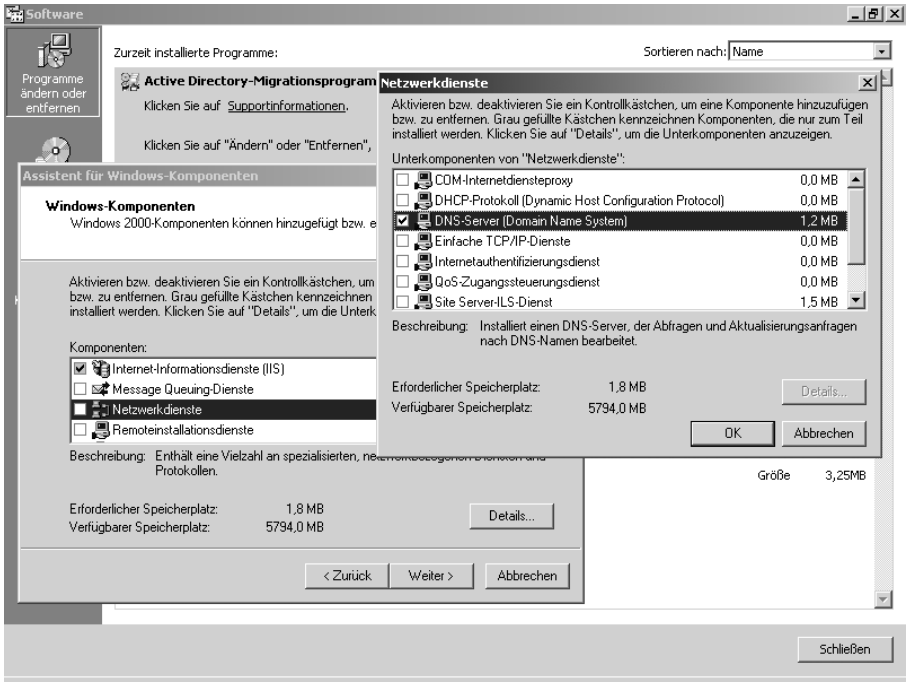
DNS muss korrekt konfiguriert werden, um die einwandfreie Funktion des Active Directory sicherzustellen. Folgende **Konfigurationselemente** sind zu überprüfen, um zu gewährleisten, dass DNS fehlerfrei eingerichtet ist und die DNS-Einträge für Active Directory korrekt registriert werden:

- DNS-Installation,
- DNS-IP-Konfiguration,

- Active Directory-DNS-Registrierung,
- dynamische Zonenaktualisierung.

4.3.1 DNS-Installation

Sofern die Netzwerkdienste für den DNS-Server noch nicht installiert sind, können sie über den Assistenten für Windows-Komponenten nachinstalliert werden.



Windows-Komponenten, Netzwerkdienste

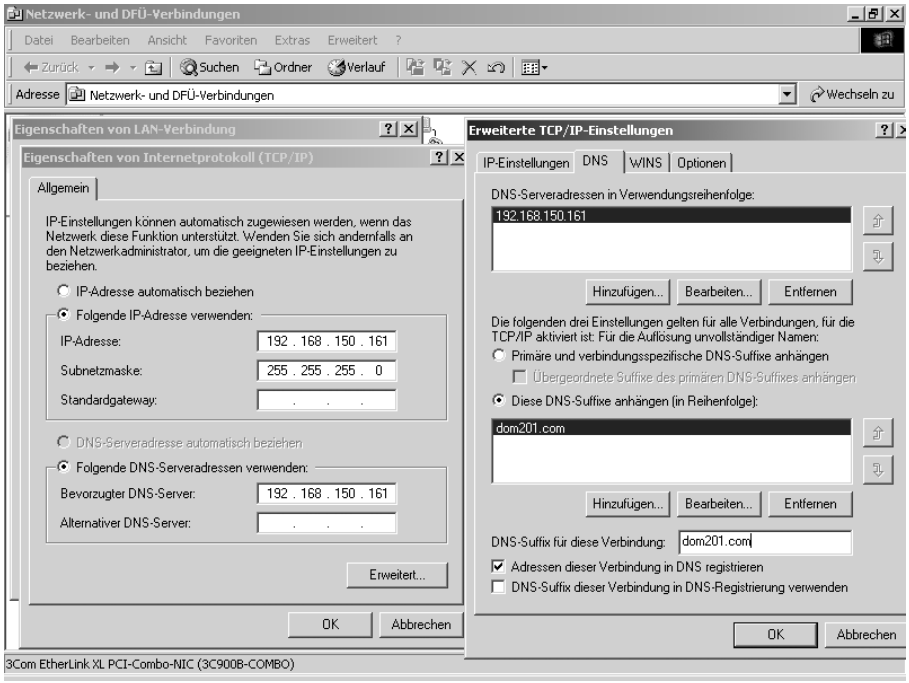
Netzwerkdienste für DNS-Server installieren!

1. *Starten Sie unter EINSTELLUNGEN-SYSTEMSTEUERUNG das Programm SOFTWARE.*
2. *Klicken Sie auf WINDOWS-KOMPONENTEN HINZUFÜGEN/ENTFERNEN.*
3. *Zeigen Sie auf NETZWERKDIENSTE und klicken Sie auf DETAILS.*
4. *Klicken Sie auf DNS-SERVER und folgen Sie den Installationsschritten.*

4.3.2 DNS-IP-Konfiguration

Die TCP/IP-Einstellungen eines Domänencontrollers, der gleichzeitig die Funktion eines DNS-Servers übernimmt, müssen korrekt konfiguriert werden. Dabei muss der Domänencontroller auf sich selbst verweisen, sodass er sich bei seinem eigenen DNS-Server registrieren kann (siehe Abbildung).

Um die aktuelle IP-Konfiguration einzusehen, öffnen Sie ein Befehlsfenster und geben Sie dort `ipconfig /all` ein, um sich die Details anzeigen zu lassen.



Eigenschaften von TCP/IP, DNS-Serveradresse

DNS-Konfiguration administrieren!

1. *Klicken Sie mit der rechten Maustaste auf NETZWERKUMGEBUNG und klicken Sie dann auf EIGENSCHAFTEN.*
2. *Klicken Sie mit der rechten Maustaste auf LAN-VERBINDUNGEN und klicken Sie dann auf EIGENSCHAFTEN.*
3. *Klicken Sie auf INTERNETPROTOKOLL (TCP/IP) und dann auf EIGENSCHAFTEN.*
4. *Klicken Sie auf ERWEITERT und dann auf die Registerkarte DNS.*
5. *Konfigurieren Sie die DNS-Serveradressen so, dass sie auf den DNS-Server*

verweisen. Falls es sich um den ersten DNS-Server handelt, müssen Sie hier die eigene IP-Adresse des Computers angeben (siehe Abbildung).

6. *Klicken Sie auf ERWEITERT, um die erweiterten TCP/IP-Einstellungen zu administrieren.*

7. *Im Fenster DNS-SERVERADRESSEN IN VERWENDUNGSREIHENFOLGE können die IP-Adressen weiterer DNS-Server angegeben werden, die für die Namensauflösung eingesetzt werden.*

8. *Im Fenster DIESE DNS-SUFFIXE ANHÄNGEN (IN REIHENFOLGE) muss der DNS-Domänenname für Active Directory zuerst aufgeführt sein (an der ersten Position in der Liste).*

9. *Stellen Sie sicher, dass die Einstellung unter DNS-SUFFIX FÜR DIESE VERBINDUNG: mit dem Active Directory-Domänennamen identisch ist.*

10. *Stellen Sie sicher, dass das Kontrollkästchen ADRESSEN DIESER VERBINDUNG IN DNS REGISTRIEREN aktiviert ist.*

11. *In der Eingabeaufforderung geben Sie* `ipconfig /flushdns` *ein, um den DNS-Auflösungscache zu leeren.*

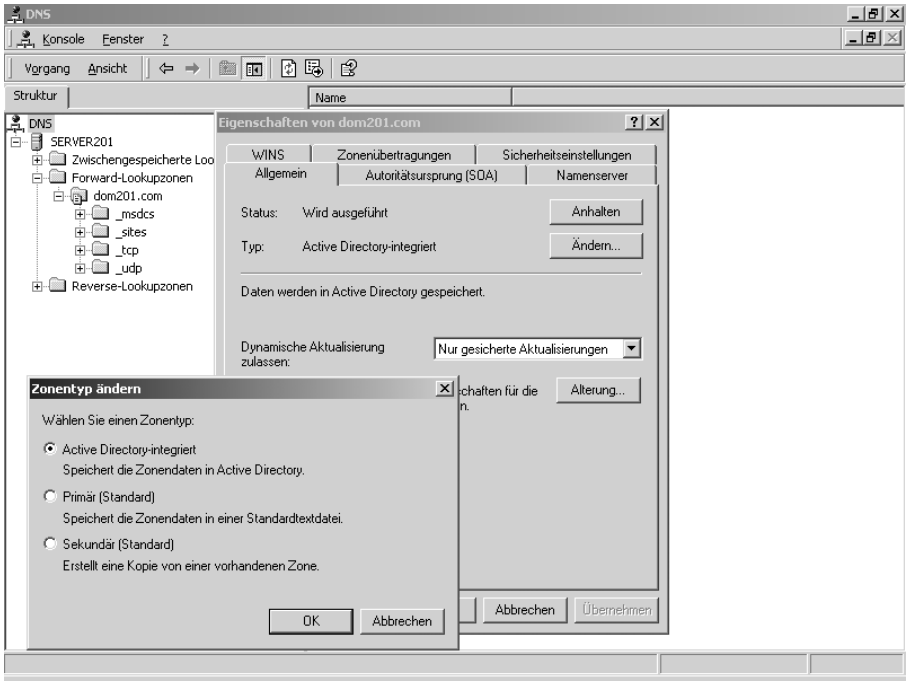
12. *Geben Sie danach* `ipconfig /registerdns` *ein, um die DNS-Ressourceneinträge registrieren zu lassen.*

Beachten Sie, dass auch auf den Clients die IP-Adresse des DNS-Servers unter INTERNETPROTOKOLL (TCP/IP)- EIGENSCHAFTEN eingetragen werden muss.

4.3.3 Active Directory-DNS-Registrierung

Die Active Directory-DNS-Einträge müssen in DNS registriert werden. Bei der DNS-Zone kann es sich entweder um eine primäre Standardzone oder eine Active Directory-integrierte Zone handeln. Eine **Active Directory-integrierte Zone** bietet die folgenden Vorteile:

- Der DNS-Dienst von Windows 2000 speichert die Zonendaten in Active Directory.
- Jeder DNS-Server kann Aktualisierungen für eine Active Directory-integrierte Zone entgegennehmen.
- Durch den Einsatz der Active Directory-Integration ist es zudem nicht mehr erforderlich, eine separate Replikationstopologie für die DNS-Zonendatenübertragung einzurichten.



DNS-Managementkonsole, Zonentyp

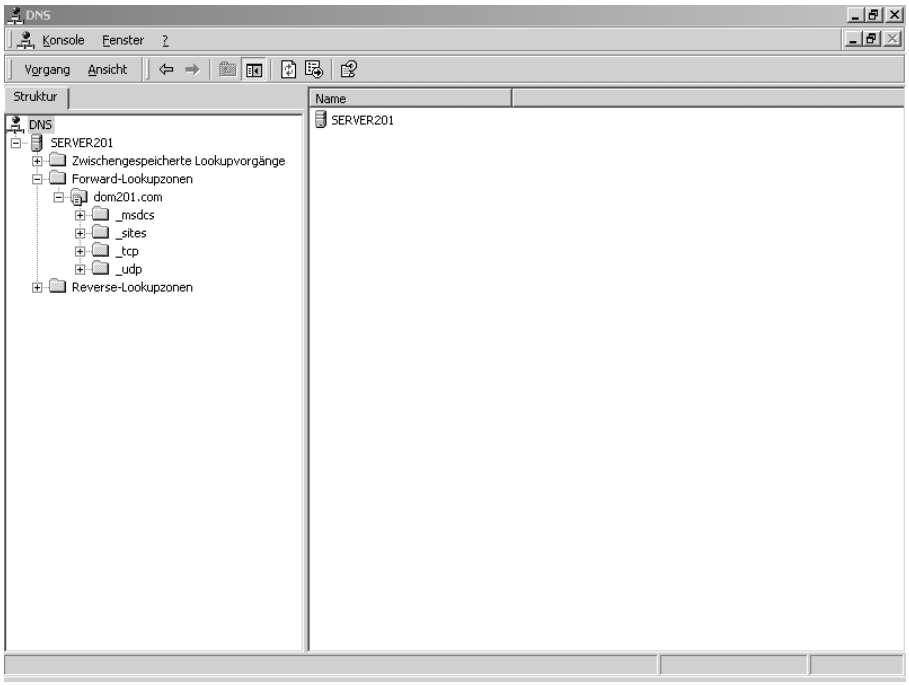
Den Zonentyp ACTIVE DIRECTORY-INTEGRIERT können Sie nur aktivieren, wenn auf dem Server bereits Active Directory eingerichtet wurde. Handelt es sich um einen Server, der nicht zum Domänencontroller heraufgestuft worden ist, können Sie entweder eine primäre Zone oder, sofern eine primäre Zone auf einem DNS-Server bereits vorhanden ist, eine sekundäre Zone auf einem zweiten DNS-Server einrichten.

Führen Sie die folgenden Schritte durch, um sicherzustellen, dass DNS die Active Directory-DNS-Einträge registriert:

Struktur der DNS-Forward-Lookupzone prüfen!

1. *Starten Sie die DNS-Managementkonsole.*
2. *Klicken Sie auf den Servernamen.*
3. *Klicken Sie auf die Option FORWARD-LOOKUPZONEN und klicken Sie dann mit der rechten Maustaste auf den Namen der DNS-Zone der Active Directory-Domäne.*
4. *Wenn DNS die Active Directory-DNS-Einträge korrekt registriert, sind vier Ordner mit den folgenden Bezeichnungen vorhanden: _msdcs, _sites, _tcp, _udp*

Falls diese Ordner nicht existieren, werden die Active Directory-DNS-Einträge nicht von DNS registriert. Diese Einträge sind für die Funktionalität des Active Directory von entscheidender Bedeutung und müssen innerhalb der DNS-Zone vorhanden sein. Sind sie nicht vorhanden, sollten Sie ggf. DNS neu installieren oder eine neue DNS-Zone erstellen (siehe Tz. 4.3.5).

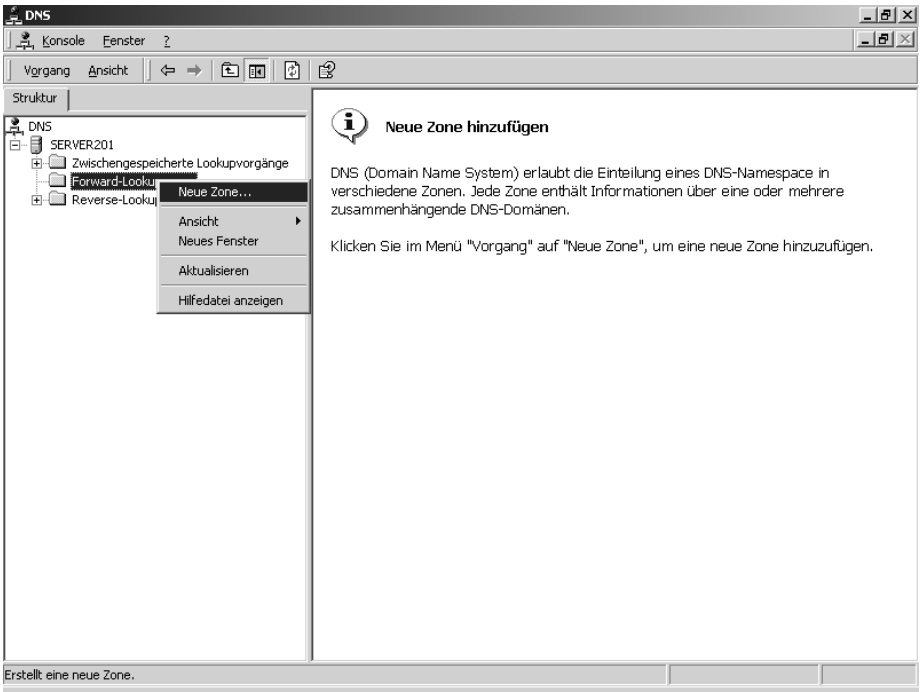


DNS-Managementkonsole, Active Directory-DNS-Einträge

Eine „neue" Forward-Lookupzone erstellen!

1. *Starten Sie die DNS-Managementkonsole.*
2. *Klicken Sie mit der rechten Maustaste auf den Namen der Zone und klicken Sie dann auf LÖSCHEN.*
3. *Falls Warnungen angezeigt werden, bestätigen Sie diese bitte, indem Sie auf OK klicken. Die gelöschte Zone wird jetzt nicht mehr unter den Forward-Lookupzonen aufgeführt.*
4. *Klicken Sie mit der rechten Maustaste auf FORWARD-LOOKUPZONEN und klicken Sie dann auf NEUE ZONE.*
5. *Der Assistent zum Erstellen neuer Zonen wird gestartet. Klicken Sie auf WEITER, um den Vorgang fortzusetzen.*
6. *Klicken Sie auf den entsprechenden Zonentyp (entweder ACTIVE DIRECTORY-INTEGRIERTE ZONE oder PRIMÄRE STANDARDZONE) und bestätigen Sie mit WEITER.*

Prüfen Sie mit *nslookup*, ob der DNS-Server Namensanfragen in IP-Adressen richtig umsetzt (siehe Tz. 4.3.5).



DNS-Managementkonsole, neue Forward-Lookupzone hinzufügen

Mithilfe einer **Reverse-Lookupzone** können IP-Adressen in Namen aufgelöst werden. Reverse-Lookupzonen sind zwar nicht zwingend erforderlich, sie werden jedoch bei der Ausführung von Fehlerbehebungs-Tools, wie beispielsweise *nslookup* (siehe Tz. 4.3.5), benötigt. Darüber hinaus implementieren verschiedene Anwendungen Sicherheitseinstellungen durch die Möglichkeit, über Namen anstelle von IP-Adressen eine Verbindung herzustellen.

Eine Reverse-Lookupzone erstellen!

1. *Starten Sie die DNS-Managementkonsole.*
2. *Klicken Sie mit der rechten Maustaste auf* REVERSE-LOOKUPZONEN *und wählen Sie* NEUE ZONE.
3. *Der Assistent zum Erstellen neuer Zonen wird gestartet. Klicken Sie auf* WEITER, *um den Vorgang fortzusetzen.*
4. *Klicken Sie auf den entsprechenden Zonentyp (entweder* ACTIVE DIRECTORY-INTEGRIERTE ZONE *oder* PRIMÄRE STANDARDZONE*) und bestätigen Sie mit* WEITER.
5. *Geben Sie unter* NETZWERKKENNUNG *die ersten drei 3er Blöcke der IP-Adresse in das Eingabefeld ein. Der Name der Reverse-Lookupzone wird im Feld* NAME

DER REVERSE-LOOKUPZONE angezeigt.

6. *Der Name der neu erstellten Zonendatei wird angezeigt. Sie können auch eine bestehende Zonendatei auswählen.*

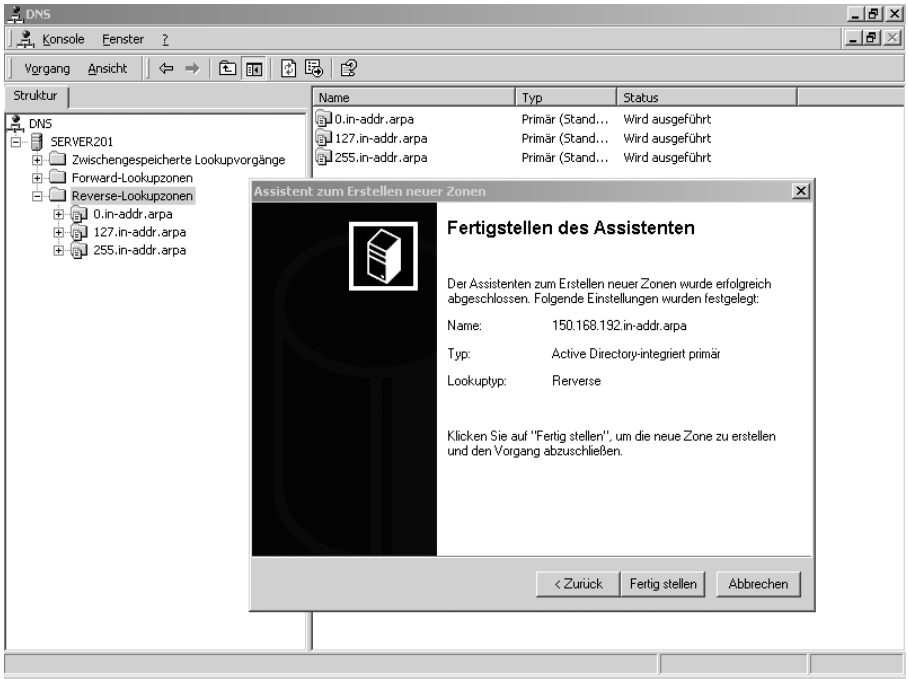
7. *Bestätigen Sie mit WEITER und danach mit FERTIGSTELLEN, um den Assistenten zu beenden. Die neu erstellte Zone erscheint jetzt in der DNS-Managementkonsole.*

8. *Geben Sie in einer Eingabeaufforderung* `net stop netlogon` *ein und drücken Sie die EINGABETASTE. Der Anmeldedienst Netlogon wird gestoppt.*

9. *Geben Sie* `net start netlogon` *ein und drücken Sie dann die EINGABETASTE. Der Anmeldedienst Netlogon wird neu gestartet.*

10. *Aktualisieren Sie die Ansicht in der DNS-Managementkonsole.*

Prüfen Sie mit *nslookup*, ob der DNS-Server IP-Adressen richtig in Hostnamen umsetzt (siehe Tz. 4.3.5).



Assistent zum Erstellen einer neuen Reverse-Lookupzone

Da die DNS-Datenbank nach Namen und nicht nach IP-Adressen indiziert wird, würde eine Reverse-Lookupabfrage einen umfangreichen Suchlauf durch sämtliche Domänennamen erfordern. Zur Lösung des Problems wurde eine spezielle Domäne erstellt, die **„in-addr.arpa“**

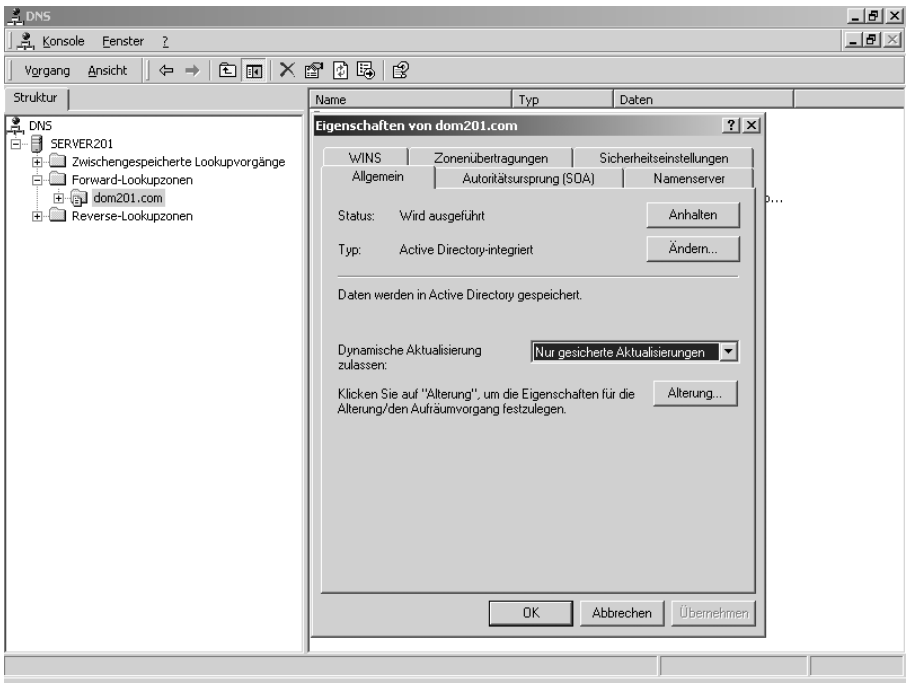
genannt wird. Eine Reverse-Lookupzone für das Subnetz 192.168.0.0/24 heißt somit 0.168.192.in-addr.arpa.

4.3.4 Dynamische Zonenaktualisierungen

Windows 2000 unterstützt die **dynamische Aktualisierung** der DNS-Datenbank. Änderungen der DNS-Einträge werden ohne administrative Eingriffe automatisch aktualisiert. Dies muss jedoch für jede Zone explizit „erlaubt“ werden.

Dynamische Aktualisierung der DNS-Datenbank administrieren!

1. *Starten Sie die DNS-Managementkonsole.*
2. *Klicken Sie mit der rechten Maustaste auf den Namen der Zone und klicken Sie dann auf EIGENSCHAFTEN.*
3. *In der Registerkarte ALLGEMEIN sollte die Einstellung für AKTUALISIERUNGEN ZULASSEN JA lauten; für eine Active Directory-integrierte Zone sollten Sie die Option JA oder die Option NUR GESICHERTE AKTUALISIERUNGEN wählen.*



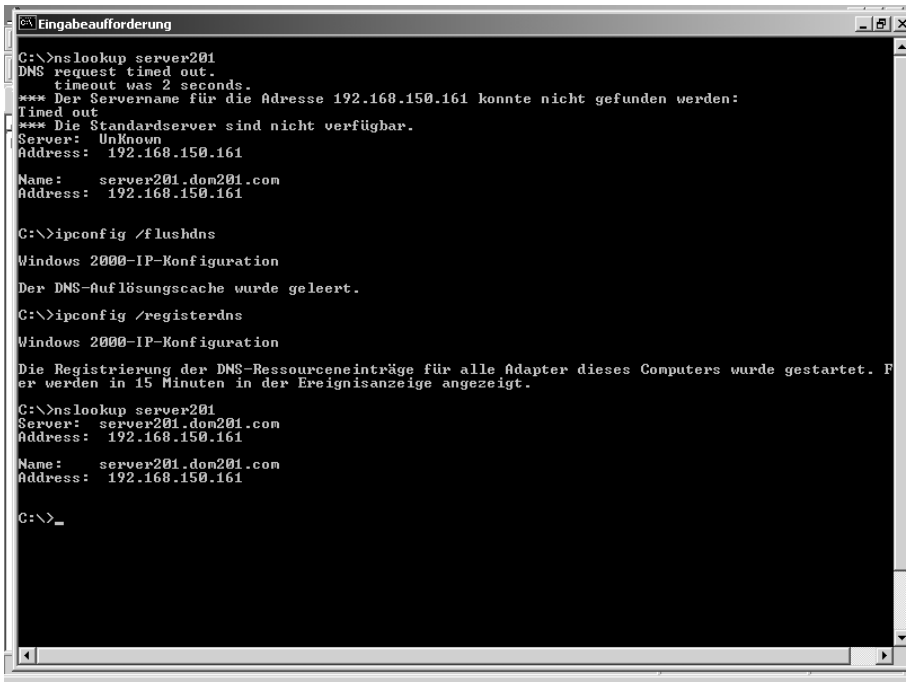
DNS-Managementkonsole, Eigenschaften der Zone dom201.com

Wenn die dynamische Aktualisierung nicht aktiviert wurde, muss die gesamte Hostregistrierung manuell durchgeführt werden.

4.3.5 DNS-Tests und Problembehandlung

Nslookup.exe ist ein Befehlszeilen-Verwaltungsprogramm für **Tests und Problembehandlung** bei DNS-Servern. Das Programm wird zusammen mit dem TCP/IP-Protokoll über die Systemsteuerung installiert. Mit *nslookup* kann über die Eingabeaufforderung u. a. die Funktionsweise eines DNS-Servers getestet werden. Sofern der DNS-Server richtig konfiguriert wurde, löst *nslookup* nach Eingabe eines Hostnamens diesen in eine IP-Adresse auf. *Nslookup* kann in zwei Modi ausgeführt werden: interaktiv und nicht interaktiv.

Der **nicht interaktive** Aufruf kann Hostnamen in Adressen oder umgekehrt Adressen in die dazugehörigen Namen auflösen. Dieser Aufruf wird verwendet, wenn nur eine einzelne Auflösung benötigt wird, z. B. `nslookup server201` (siehe nachfolgende Abbildung).



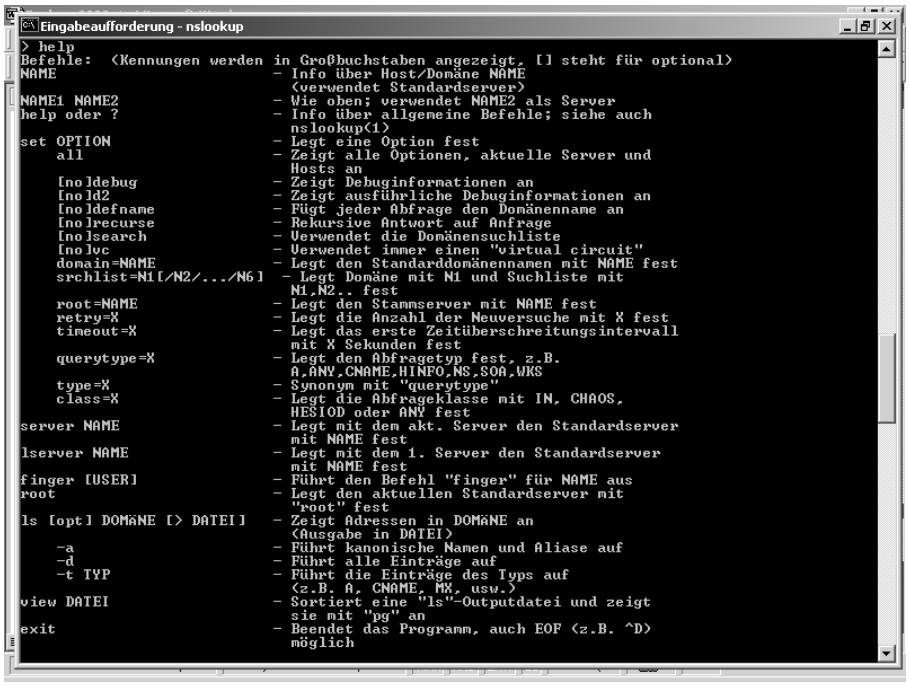
Nicht interaktive Abfragen mit nslookup

Beachten Sie, dass *nslookup* nur dann die Übersetzung in Hostname bzw. IP-Adresse richtig anzeigt, wenn eine **Forward- und Reverse-Lookupzone** korrekt eingerichtet wurde. Fehlt beispielsweise die Reverse-Lookupzone, kann der Ser-

vername über die IP-Adresse nicht aufgelöst werden. Entsprechend gibt *nslookup* eine **Fehlermeldung** aus (siehe nslookup-Abfrage in der Abbildung).

Sofern Sie eine neue Lookupzone erstellen, löschen oder ändern, sollten Sie den DNS-Cache mit den Befehlen `ipconfig /flushdns` (Cacheleerung) und `ipconfig /registerdns` (DNS-Register in Cache übertragen) aktualisieren (siehe Abbildung). Erst danach kann *nslookup* die aktuellen DNS-Daten übersetzen.

Der **interaktive** Aufruf wird verwendet, wenn nicht nur eine einzige Adresse aufgelöst werden soll. Nach Aufruf von nslookup gelangt man in den **Befehlszeilenmodus** von nslookup. Unter diesem Modus können die entsprechenden DNS-Befehle eingegeben werden.



nslookup – help

Nslookup im interaktiven Modus verwenden!

1. *Um nslookup im interaktiven Modus zu starten, geben Sie* `nslookup` *in der Eingabeaufforderung ein. Es erscheint der Befehlszeilenmodus, z. B.:*
   C:\> nslookup
   Standardserver: nameserver1.domain.com
   Adresse: 10.0.0.1
   >

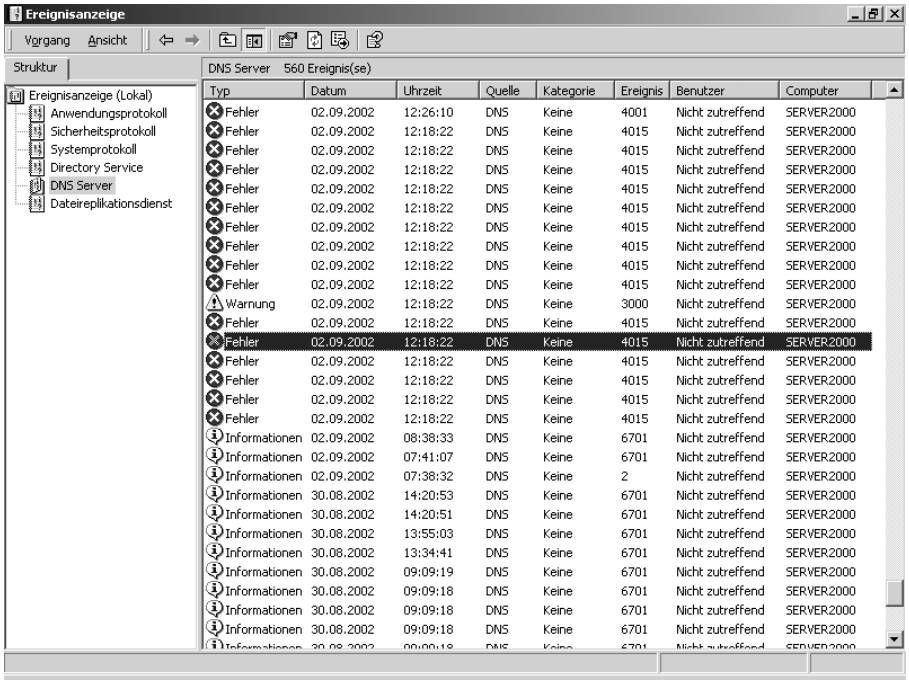
2. *Alle Angaben in der Eingabeaufforderung, die nicht als gültiger Befehl erkannt werden, werden als Hostname interpretiert, und das System versucht, den Namen über den DNS-Server aufzulösen.*

3. *Durch Eingabe von* `help` *oder* `?` *in der Eingabeaufforderung erhalten Sie eine Liste der verfügbaren Befehle.*

4. *Interaktive Befehle können Sie mit STRG+C unterbrechen.*

5. *Um den interaktiven Modus zu verlassen und auf die Eingabeaufforderung zurückzukehren, geben Sie* `exit` *in der Eingabeaufforderung ein.*

Arbeitet der DNS-Server nicht korrekt, sollte in der **Ereignisanzeige** das Protokoll für den DNS-Server überprüft werden. Über die mit Fehler gekennzeichneten Einträge kann ggf. die Ursache für die Fehlerquelle analysiert werden.



Ereignisanzeige – DNS-Server-Protokolleinträge

Protokoll der Ereignisanzeige überprüfen!

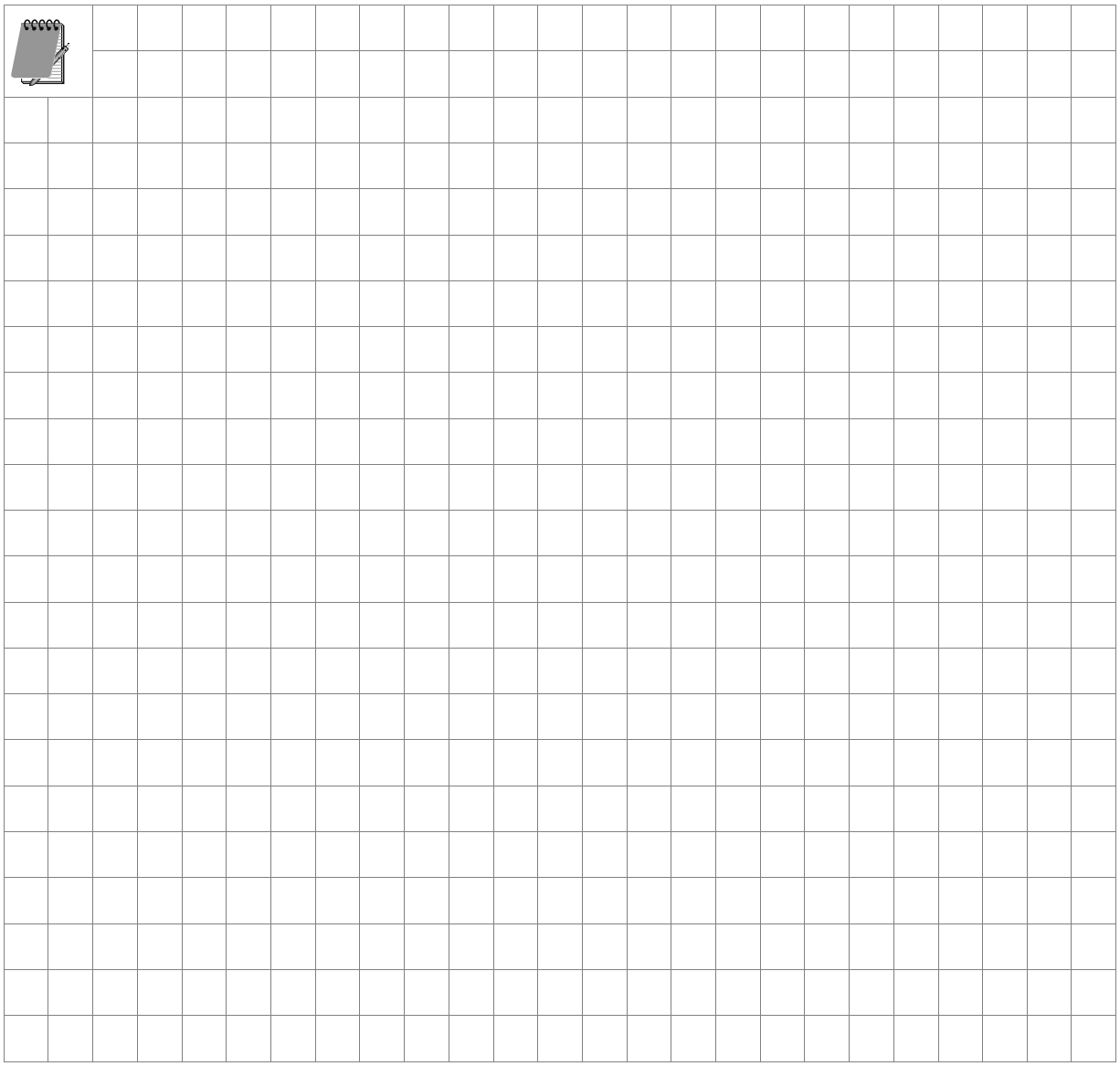
1. *Zum Öffnen der Ereignisanzeige klicken Sie auf* START*, zeigen auf* EINSTELLUNGEN *und klicken auf* SYSTEMSTEUERUNG*.*

2. *Doppelklicken Sie auf* VERWALTUNG *und anschließend auf* EREIGNISANZEIGE*.*

3. *Zeigen Sie auf DNS-Server und überprüfen Sie die Protokolleinträge.*

4.4 Sicherheitscheck

- *Die richtige **Funktionsweise** des Domain Name System (DNS) ist Grundvoraussetzung für den Einsatz des Active Directory.*
- *Die Installation und Konfiguration von DNS sind abhängig von der **Größe** der Domänengesamtstruktur (siehe Kapitel 5).*
- *Erstellen Sie Forward- und Reverse-Lookupzonen als **Active Directory-integriert mit dynamischer Aktualisierung**, um die Replikation der DNS-Zonendaten mit dem Active Directory zu verbinden.*
- *Da der DNS-Server über elementare Informationen verfügt, sollten Sie sicherstellen, dass die DNS-Zonendaten **redundant** verwaltet werden (siehe Kapitel 5).*



5 Active Directory

In diesem Kapitel erfahren Sie,

- wie das Active Directory strukturiert ist,
- was bei der Installation des Active Directory beachtet werden sollte,
- welche Verwaltungsprogramme für die Administration des Active Directory zur Verfügung stehen,
- welche Bedeutung Organisationseinheiten im Active Directory haben,
- welche Active Directory-Objekte zur Verfügung stehen,
- wie Aufgaben für die Administration des Active Directory über Berechtigungen zugewiesen werden können,
- wie von einem Client aus das Active Directory administriert werden kann,
- was unter einem *Standort* zu verstehen ist und
- wann eine Replikation des Active Directory erfolgt.

5.1 Planen der Active Directory-Implementierung

Vor der **Implementierung** einer Windows 2000-Netzwerkumgebung ist festzulegen, wie das Active Directory eingerichtet werden soll. Bei der Planung sollten die **Organisationsstrukturen** berücksichtigt werden. Dazu gehören Bürostandorte bzw. Außenstellen, eventuelle Organisationsveränderungen und der Zugriff auf die Netzwerkressourcen. Des Weiteren sollten auch die Administrationsanforderungen berücksichtigt werden. Außerdem muss das Modell skalierbar und erweiterbar sein, um Änderungen in der Organisationsstruktur übernehmen zu können.

Zunächst ist der **DNS-Namensraum** (DNS-Namespace) festzulegen. Ein DNS-Namensraum ist ein Domänenname der obersten Ebene im Active Directory (siehe Kapitel 4). An den Namensraum sind die Domänenhierarchie, Vertrauensstellungen und die Replikation geknüpft.

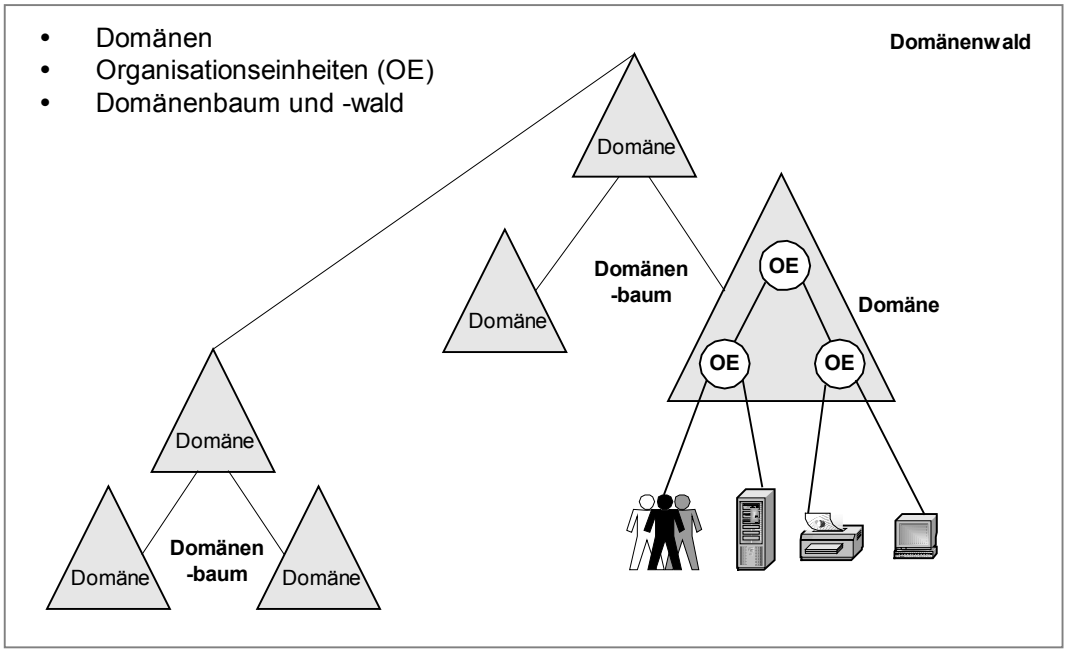
Beim Implementieren der Active Directory-Dienste gibt es zwei Möglichkeiten für die Festlegung des Namensraums. Entweder wird der DNS-Namensraum nach einem durch die Organisation bereits registrierten **externen** Internet-DNS-Namensraum oder als **eigenständiger** losgelöster DNS-Namensraum vergeben.

Es gibt bei beiden Modellen Vor- und Nachteile. Im Ergebnis wird aber der Administrationsaufwand bei identischem internen und externen DNS-Namensraum erheblich höher sein.

Die logische Struktur des Active Directory ist eine **Baumstruktur**, die eine Abbildung einer gesamten Organisation ermöglicht. Sie umfasst folgende Elemente:

Domänenwald bzw. Domänengesamtstruktur	=	Forest
Domänenbaum	=	Domain Tree
Domäne	=	Domain
Organisationseinheiten (OE)	=	Organization Units (OU)

Die erste Windows 2000-Domäne ist eine so genannte *Root-Domäne*. Sie enthält alle *Betriebsmasterfunktionen* sowie den G*lobalen Katalog* (siehe Kapitel 3). Weitere untergeordnete Domänen bilden den ersten Domänenbaum *(Domain Tree)*. Die Einrichtung eines zweiten Domänenbaums erzwingt die Erweiterung des Namensraums. Mehrere Domänenbäume bilden dann einen so genannten Domänenwald *(Forest)*.



Domänen, Domänenbaum und –wald

Mehrere Domänen im gleichen DNS-Namensraum (Namespace) bilden einen Domänenbaum. Ein Domänenwald ist eine Gruppe von Domänenbäumen mit unterschiedlichen DNS-Namensräumen. Alle Domänenbäume nutzen jedoch das *Schema*, die *Konfiguration* sowie den *Globalen Katalog* der Root-Domäne.

Mit der Einrichtung einer neuen Domäne innerhalb einer Domänengesamtstruktur werden automatisch bidirektionale, transitive Vertrauensstellungen hergestellt (siehe Kapitel 2).

5.2 Active Directory-Datenbank

Die Active Directory-Datenbank ist das Verzeichnis für die neue Domäne. In dem Verzeichnis bzw. in der hierarchischen Datenbank eines jeden Domänencontrollers (DC) werden die Verzeichnisobjekte Benutzer, Gruppen, Computer, Drucker, Freigaben und Dienste gespeichert. Änderungen werden zwischen allen Domänencontrollern innerhalb der Domäne und der Domänengesamtstruktur repliziert und stehen somit den Benutzern und Applikationen im Netzwerk zur Verfügung.

Der standardmäßige **Speicherort** für die Datenbank und die Datenbankprotokolldateien lautet **Stammverzeichnis:\ntds**. Der Ordner muss sich auf einer Partition oder einem Datenträger befinden, der mit dem Dateisystem *NTFS* formatiert wurde. Er kann aber während der Installation des Active Directory geändert werden. Aufgrund der wachsenden Größe der Datenbank und des ständigen Zugriffs kann eine bessere Performance erzielt werden, wenn die Datenbank und die Protokolldateien auf separaten Datenträgern bzw. Festplatten mit einer RAID-Implementation (Redundant Array of Independent Disks) gespeichert werden. Damit wird zugleich eine höhere Verfügbarkeit der elementaren Active Directory-Daten erreicht.

Die Datenbank wird in einer Datei mit dem Namen *Ntds.dit* gespeichert. Sie enthält alle Informationen, die im Active Directory enthalten sind. Dazu gehören das gesamte *Schema*, der *Globale Katalog* sowie alle Objekte, die auf dem Domänencontroller gespeichert werden. Während des Heraufstufens zum Domänencontroller wird die Datei *Ntds.dit* vom Verzeichnis bzw. Ordner **Stammverzeichnis:\System32** in das angegebene Verzeichnis kopiert. Die Active Directory-Dienste werden anschließend von der Datenbank gestartet. Falls andere Domänencontroller vorhanden sind, wird die Datei durch die Replikation aktualisiert.

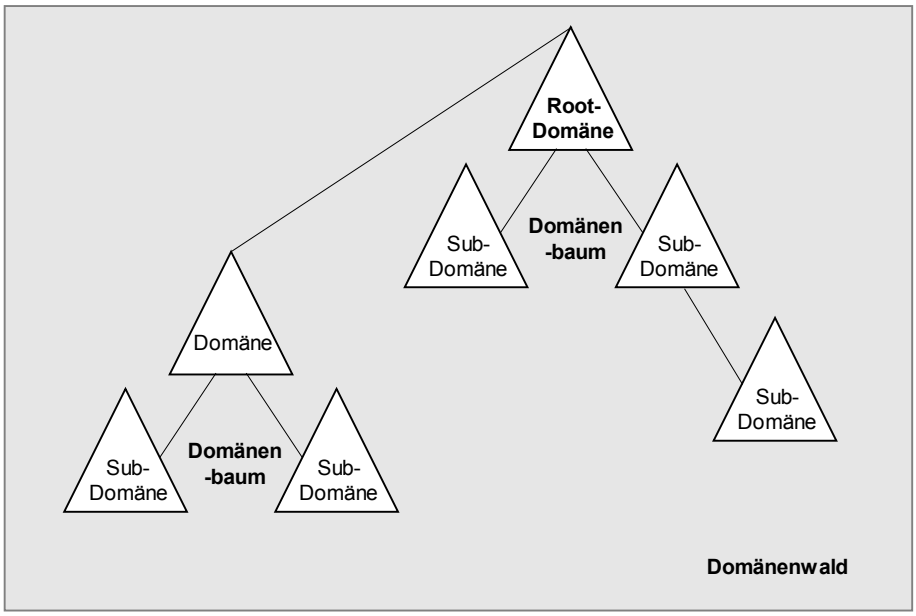
Das Verzeichnis bzw. der Ordner **Sysvol** ist ebenfalls ein Bestandteil des Active Directory. In dem Ordner werden Skripte und einige der Gruppenrichtlinienobjekte für die aktuelle Domä-

ne gespeichert. Der standardmäßige Speicherort für den freigegebenen Ordner lautet **Stammverzeichnis:\Sysvol**. Der Ordner muss sich ebenfalls auf einer Partition oder einem Datenträger befinden, der mit dem Dateisystem *NTFS* formatiert wurde.

5.3 Installation

Nach der Installation von Windows 2000 Server wird das Active Directory **nicht** automatisch installiert. Erst über das Programm *dcpromo* kann es auf dem Server folgendermaßen eingerichtet werden:

- Erstellung der ersten **Root-Domäne** (erste Domäne in der Gesamtstruktur bzw. im Forest) und gleichzeitig die Einrichtung des ersten Domänencontrollers,
- Erstellung eines **zusätzlichen** Domänencontrollers (Replikationscontroller) in einer bestehenden Domäne,
- Erstellung einer weiteren **Sub- bzw. Child-Domäne** und gleichzeitig die Einrichtung des ersten Domänencontrollers in der neuen Domäne,
- Erstellung eines **neuen** Domänenbaums innerhalb der Domänengesamtstruktur (Domänenwald) und gleichzeitig die Einrichtung des ersten Domänencontrollers.



Domänenstruktur

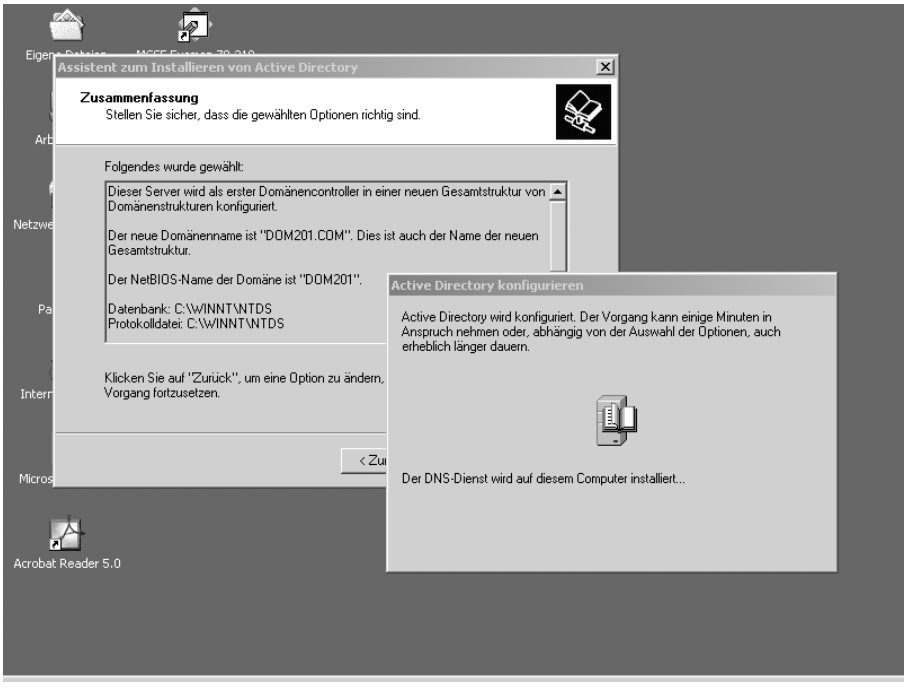
Die erste Root-Domäne hat eine Sonderstellung, da sie die Gruppen *Schema-Admins* und *Organisations-Admins* enthält (siehe Kapitel 6).

Für die volle Funktionsweise des Active Directory wird ein DNS-Server benötigt. Dieser wird mit der Installation von Active Directory in der Regel automatisch installiert, wenn noch kein DNS-Server vorhanden ist (siehe Kapitel 4).

Folgendes ist bei der Installation des Active Directory zu beachten:

Wenn Sie das Active Directory für eine größere Organisation installieren, sollten Sie vorher einen Implementierungsplan erstellen. Dieser Plan sollte alle notwendigen Informationen über die gesamte Netzwerk- und Organisationsstruktur enthalten.

Ist DNS nicht ordnungsgemäß konfiguriert, werden einzelne Bereiche des Active Directory, wie z. B. die Umsetzung der Gruppenrichtlinien, nicht unterstützt. Es ist deshalb zu empfehlen, zunächst die Einstellungen des DNS zu überprüfen (siehe Kapitel 4).



Active Directory installieren

Domänencontroller in einer neuen Gesamtstruktur installieren!

1. *Klicken Sie auf START-AUSFÜHREN, geben Sie* `dcpromo` *ein und bestätigen Sie anschließend mit OK.*

2. *Hierdurch wird der Assistent für die Installation von Active Directory gestartet. Klicken Sie auf WEITER.*

3. *Da Sie den Server als den ersten Domänencontroller in der Gesamtstruktur installieren, wählen Sie DOMÄNENCONTROLLER FÜR EINE NEUE DOMÄNE und klicken dann auf WEITER.*

4. *Da dieser Domänencontroller zudem der erste Domänencontroller in einer neuen Domänenstruktur sein wird, wählen Sie EINE NEUE DOMÄNENSTRUKTUR ERSTELLEN und klicken danach auf WEITER.*

5. *Klicken Sie AUF NEUE GESAMTSTRUKTUR AUS DOMÄNENSTRUKTUREN ERSTELLEN und danach auf WEITER.*

6. *Geben Sie im Fenster NAME DER NEUEN DOMÄNE den vollständigen DNS-Namen für die neue Domäne als voll qualifizierten Domänennamen (Beispiel: Microsoft.com) ein. Nach der Eingabe klicken Sie auf WEITER. (Im Fenster NETBIOS-DOMÄNENNAME wird im Feld NETBIOS-NAME der erste Teil des voll qualifizierten Domänennamens (Beispiel: Microsoft) eingetragen.*

7. *In den Dialogfeldern DATENBANK: und PROTOKOLLDATEI: ist das Standardverzeichnis <Stammverzeichnis:\Winnt\Ntds> eingetragen. Um eine hohe Performance und die Wiederherstellbarkeit zu gewährleisten, sollten Sie die Datenbank auf einer anderen Festplatte speichern als die Protokolldateien. Der Datenträger muss jedoch das NTFS-Dateisystem verwenden.*

8. *Ändern Sie ggf. die Eintragungen für die Datenbank und für die Protokolldatei so, dass beide Dateien auf separaten Festplatten oder zumindest auf eigenständigen Partitionen gespeichert werden. Klicken Sie auf WEITER.*

9. *Im Fenster FREIGEGEBENES SYSVOL wird als Standardverzeichnis <Stammverzeichnis:\Winnt\Sysvol> vorgegeben. Hierfür sollte ebenfalls ein eigener Speicherbereich auf einem NTFS-Datenträger (Festplatte oder Partition) eingerichtet werden. Ändern Sie ggf. die Einstellungen und klicken Sie auf WEITER.*

10. *Wenn kein DNS-Server verfügbar ist, wird die folgende Meldung angezeigt: „Eine Verbindung mit dem DNS-Server, der für den Namen <Domänenname> zuständig ist, konnte nicht hergestellt werden. Es konnte nicht festgestellt werden, ob die dynamische Aktualisierung unterstützt wird. Bestätigen Sie die DNS-Konfiguration, oder installieren oder konfigurieren Sie einen DNS-Server auf diesem Computer.“ Bestätigen Sie mit OK.*

11. *Wählen Sie JA, DNS AUF DIESEM COMPUTER INSTALLIEREN UND KONFIGURIEREN (EMPFOHLEN). Klicken Sie auf WEITER.*

12. *Geben Sie im Fenster ADMINISTRATORKENNWORT FÜR VERZEICHNISDIENSTE WIEDERHERSTELLEN das Administratorkennwort an, das Sie zum Starten des Computers im Modus VERZEICHNISDIENSTE WIEDERHERSTELLEN verwenden. Der Modus VERZEICHNISDIENSTE WIEDERHERSTELLEN dient dazu, die Active Directory-Datenbank wiederherzustellen.*

13. *Bestätigen Sie im Fenster ZUSAMMENFASSUNG die von Ihnen ausgewählten Optionen und klicken Sie anschließend auf WEITER.*

14. *Nachdem das Active Directory installiert ist, klicken Sie auf BEENDEN, um den Assistenten zu schließen. Starten Sie den Computer neu.*

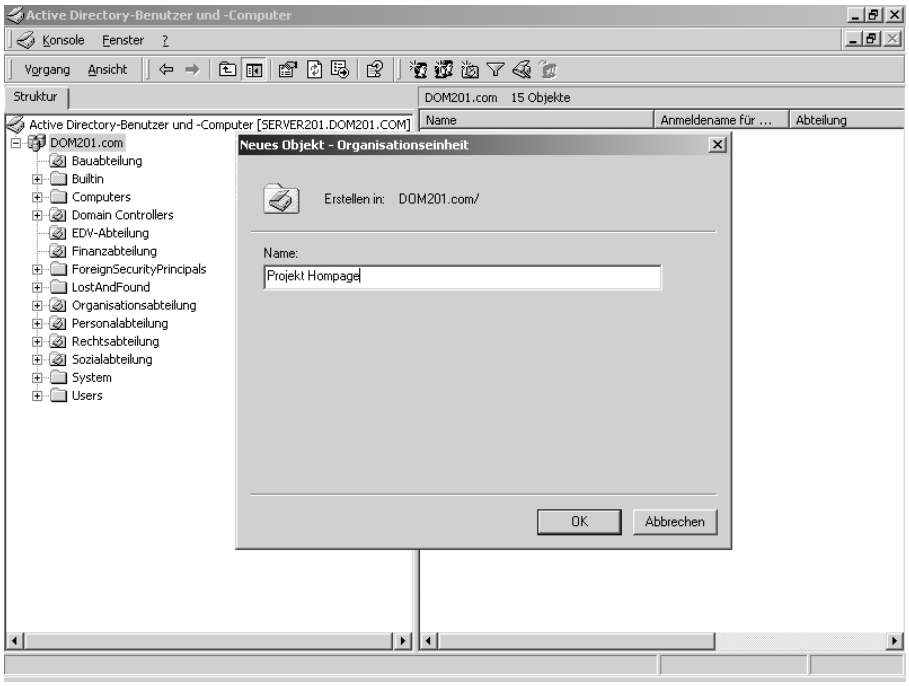
Das Administratorkennwort für die Wiederherstellung der Verzeichnisdienste sollten Sie sich aufschreiben und an einem sicheren Ort verwahren. Im Falle einer Beschädigung des Active Directory wird es für die Wiederherstellung bzw. für die Reparatur benötigt. Das Kennwort ist eigenständig. Es ist nicht mit dem Kennwort des Administratorbenutzerkontos zu verwechseln.

Nach der Installation des Domänencontrollers stehen zusätzlich folgende Standard-Verwaltungsprogramme für das Active Directory zur Verfügung:

- Active Directory-Benutzer und -Computer,
- Active Directory-Domänen und -Vertrauensstellungen sowie
- Active Directory-Standorte und -Dienste.

5.4 Organisationseinheiten (OE)

Nach der Installation des Active Directory ist es notwendig, Strukturen zu schaffen, die die Administration der Systeme vereinfachen und die Datensicherheit erhöhen. Mithilfe so genannter **Organisationseinheiten** (OE) lassen sich Domänen strukturieren. Sie können hierarchisch angeordnet und ineinander verschachtelt werden. Mit dem Entwurf der OE-Struktur wird in erster Linie das **Verwaltungsmodell** für das Active Directory festgelegt. Es können über Zugriffsrechte Zuständigkeiten für die Verwaltung einzelner Objekte (Benutzer, Gruppen usw.) vergeben werden. Außerdem können den einzelnen OE (Abteilungen) **Gruppenrichtlinien** zugewiesen werden, sodass die (z. B. von den Abteilungen) festgelegten **Sicherheitsanforderungen** differenziert zugeordnet werden können.



Active Directory-Benutzer und –Computer – Neues OE-Objekt

Eine OE kann folgende Objekte enthalten:

- Benutzer,
- Gruppen,
- Computer,
- Drucker,
- Sicherheitsrichtlinien,
- Dateifreigaben,
- Applikationen und
- untergeordnete OE.

Bei der Verwaltung von OE sind folgende Regeln zu beachten:

- *Erstellen Sie OE zum Delegieren von administrativen Verwaltungsaufgaben.*
- *Entscheiden Sie, wer welche Benutzer, Gruppen und sonstigen Ressourcen administrieren soll.*

- *Realisieren Sie eine logische und aussagekräftige OE-Struktur, sodass OE-Administratoren ihre Aufgaben effizient durchführen können.*
- *Vermeiden Sie das Zuweisen zu vieler untergeordneter Objekte innerhalb einer OE.*
- *Erstellen Sie OE zum Anwenden von Gruppen- bzw. Sicherheitsrichtlinien.*

Erstellen einer Organisationseinheit!

1. *Klicken Sie auf START-PROGRAMME-VERWALTUNG und wählen Sie ACTIVE DIRECTORY-BENUTZER UND -COMPUTER.*
2. *Klicken Sie mit der rechten Maustaste auf das Domänenobjekt oder eine andere Organisationseinheit, in der Sie eine Organisationseinheit erstellen wollen.*
3. *Zeigen Sie auf NEU und klicken Sie anschließend auf ORGANISATIONSEINHEIT.*
4. *Geben Sie im Eingabefeld NAME den Namen für das neue Objekt ein und klicken Sie anschließend auf OK. Ein Symbol mit dem entsprechenden Namen wird erstellt und in die Liste eingefügt.*
5. *Sie können nun andere Objekte wie Benutzer, Gruppen, Computer und weitere Organisationseinheiten zu der Organisationseinheit hinzufügen.*

Für eine **mittelgroße Organisation** könnte die Active Directory-Struktur **beispielsweise** folgendermaßen aussehen:

- Die Root-Domäne erhält den Namen der Organisation.
- Für die Replikation der Active Directory-Datenbank wird ein weiterer Domänencontroller eingerichtet.
- Die Abteilungen der Organisation werden im Active Directory durch das Anlegen von OE dargestellt, ggf. werden untergeordnete OE eingerichtet, die die Namen der Unterabteilungen erhalten.
- Den einzelnen OE werden die Objekte (z. B. Benutzer-, Gruppenkonten und Gruppenrichtlinien) zugeordnet.
- Es werden ggf. auf der OE-Ebene differenzierte Berechtigungen für Administratoren vergeben.

5.5 Active Directory-Objektverwaltung

Mit dem Verwaltungsprogramm *Active Directory-Benutzer und -Computer* können Objekte im Active Directory verwaltet werden. Dem Administrator stehen für die Objektbearbeitung verschiedene Funktionen (wie z. B. Suchen, Löschen, Anlegen oder Verschieben) zur Verfügung. Nach der Installation des Active Directory werden von Windows 2000 folgende Objekte angelegt (die Option ANSICHT-ERWEITERTE FUNKTIONEN muss aktiviert sein, damit alle unten aufgeführten Objekte angezeigt werden):

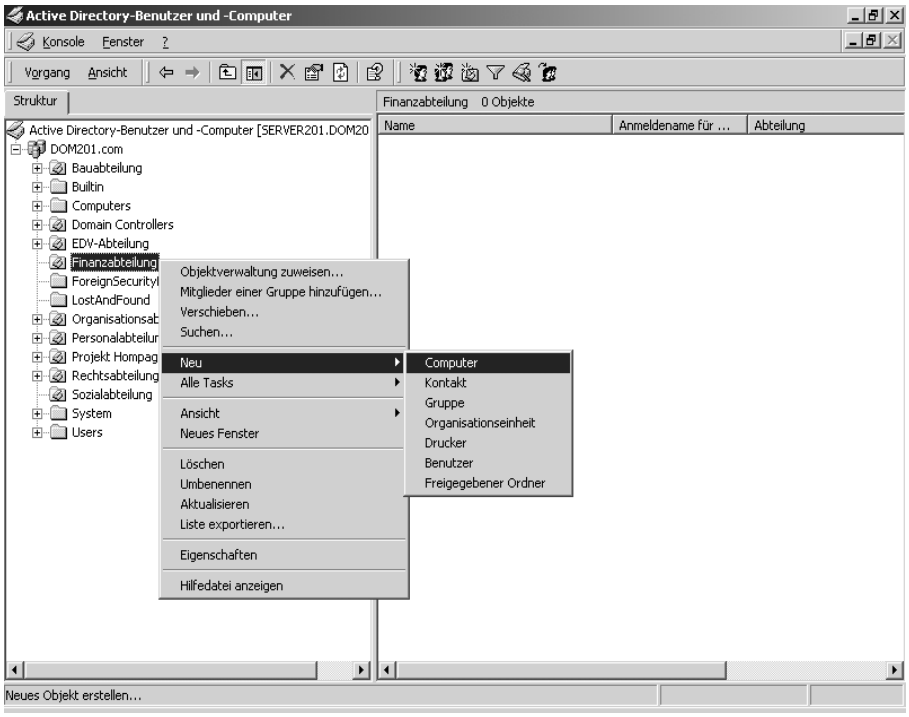
- Builtin,
- Computers,
- ForeignSecurityPrinzipals,
- LostAndFound,
- System,
- Users.

Diese vordefinierten Objekte werden im Active Directory als *Container* bezeichnet, sind aber wie Organisationseinheiten zu verstehen (siehe Kapitel 6). Zu berücksichtigen ist jedoch, dass die vordefinierten *Container/OE* administrativ nicht gelöscht oder in andere OE verschoben werden können. Über die rechte Maustaste können jedoch weitere Objekte innerhalb der *Container* hinzugefügt, gelöscht, verschoben oder umbenannt werden.

Die vordefinierten *Container* können auch am Ordnersymbol erkannt werden. Es enthält im Gegensatz zu den *OE* kein „geöffnetes Buch“.

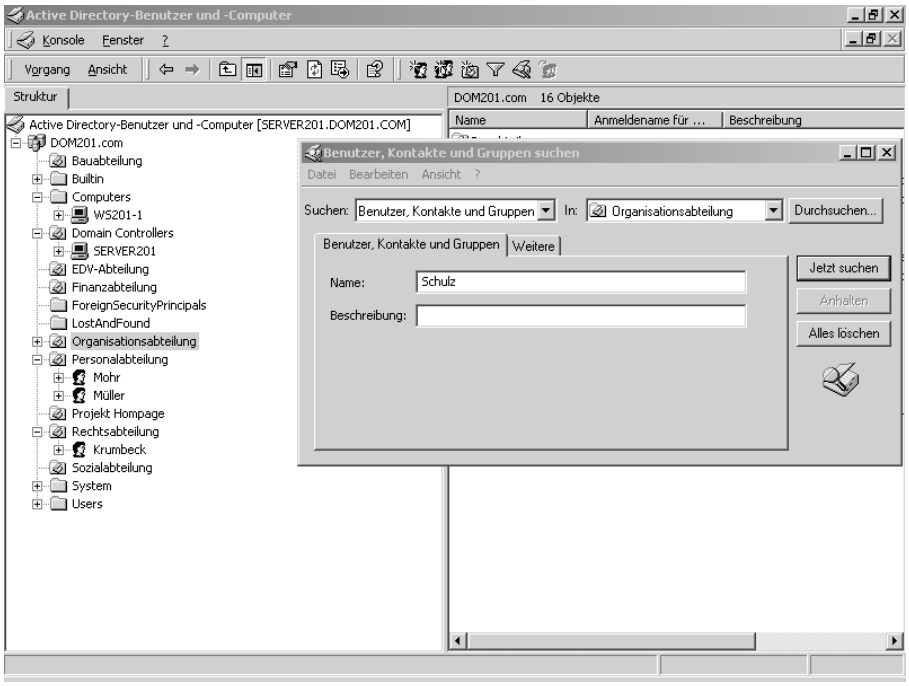
Active Directory-Objekte	**Beschreibung**
Benutzer	Die in diesem Objekt gespeicherten Informationen erlauben einem Benutzer sich an der Domäne anzumelden. Das Objekt besitzt viele optionale Felder, u. a. Vorname, Name, Telefonnummer und E-Mail-Adresse.
Gruppe	Diesem Objekt werden insbesondere Benutzerkonten zugewiesen, um z. B. die Administration der Rechtezuweisung zu vereinfachen.

Organisationseinheit	Mit den OE-Objekten wird das Active Directory strukturiert.
Computer	Dieses Objekt enthält Informationen über einen Computer, der Mitglied der Domäne ist.
Drucker	Das Objekt *Drucker* richtet eine Verknüpfung zu einem unter Windows 2000 eingerichteten Drucker ein.
Freigegebener Ordner	Das Objekt *Freigegebener Ordner* stellt eine Verknüpfung mit einem in der Domäne verfügbaren Ordner dar.
Kontakt	Das Objekt *Kontakt* enthält Informationen über Name, Vorname und Anzeigename.



Active Directory-Benutzer und -Computer – Neues Objekt anlegen

Damit einzelne Objekte in einer komplex angelegten Active Directory-Struktur auch gefunden werden können, verfügt das Verwaltungsprogramm über eine **Suchfunktion**. Das Durchsuchen nach bestimmten Informationen kann je nach Umfang der Organisationsstruktur sehr lange dauern. Deshalb wird für die effektive Abarbeitung eines Suchvorganges auf den *Globalen Katalog* zugegriffen. Der *Globale Katalog* dient aber nicht nur für das „schnelle“ Auffinden von Objekten (siehe Kapitel 3).



Active Directory-Benutzer und -Computer – Objekt suchen

Hinzufügen eines Objektes!

1. *Klicken Sie auf Start-Programme-Verwaltung und wählen Sie Active Directory-Benutzer und -Computer.*
2. *Klicken Sie mit der rechten Maustaste auf die Domäne oder auf eine vorhandene OE, in der Sie ein neues Objekt hinzufügen wollen.*
3. *Zeigen Sie auf NEU und danach auf eines der aufgelisteten Objekte.*
4. *Klicken Sie auf das Objekt und folgen Sie den weiteren Eingabefeldern.*

Verschieben eines Objektes!

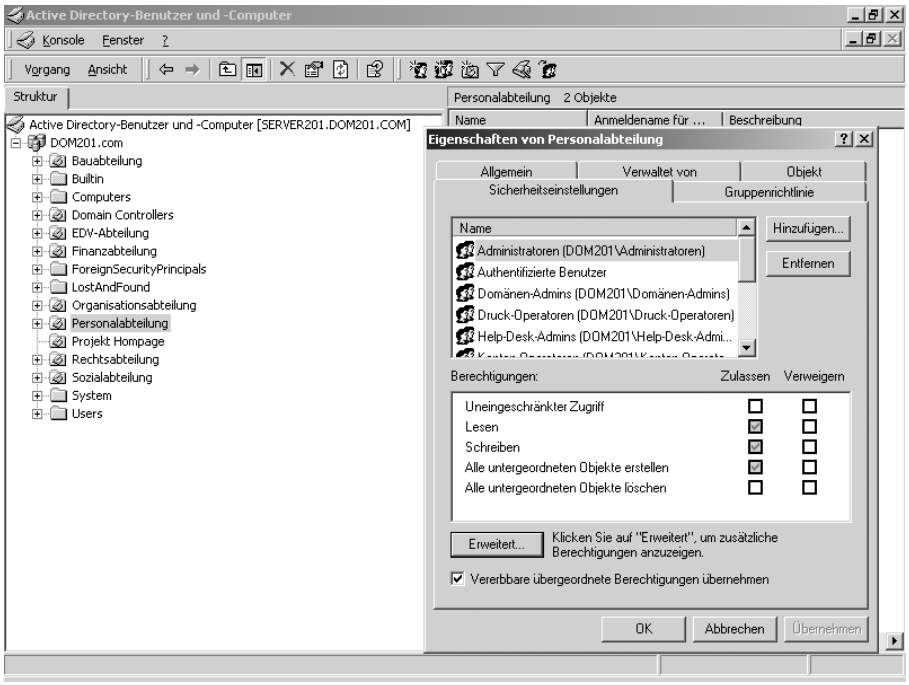
1. *Markieren Sie mit der linken Maustaste das Objekt, das verschoben werden soll.*
2. *Klicken Sie dann mit der rechten Maustaste auf das markierte Objekt und wählen Sie VERSCHIEBEN. Es öffnet sich das Fenster VERSCHIEBEN.*
3. *Zeigen Sie auf den Container (OE), in den das Objekt verschoben werden soll.*
4. *Klicken Sie auf den Container (OE) und danach auf OK.*

5.6 Active Directory-Berechtigungen

Die Zuweisung von Administrationsrechten im Active Directory ist dann sinnvoll, wenn die **Aufgaben der Administratoren** in Bezug auf die Verwaltung des Active Directory verteilt werden sollen. Auf den ersten Blick wirkt die Vergabe von Berechtigungen im Active Directory einfach. Mithilfe des **Assistenten** können den Benutzern bzw. Administratoren in einfacher Weise auf alle Objekte Berechtigungen zugewiesen werden. Bei näherer Betrachtung verbirgt sich dahinter aber ein ausgesprochen komplexes Modell. Die Erteilung von Berechtigungen im Active Directory kann auf der Ebene

- der Domäne,
- der Organisationseinheiten sowie
- der einzelnen Objekte

erfolgen.



Sicherheitseinstellungen der OE „Eigenschaften von Personalabteilung“

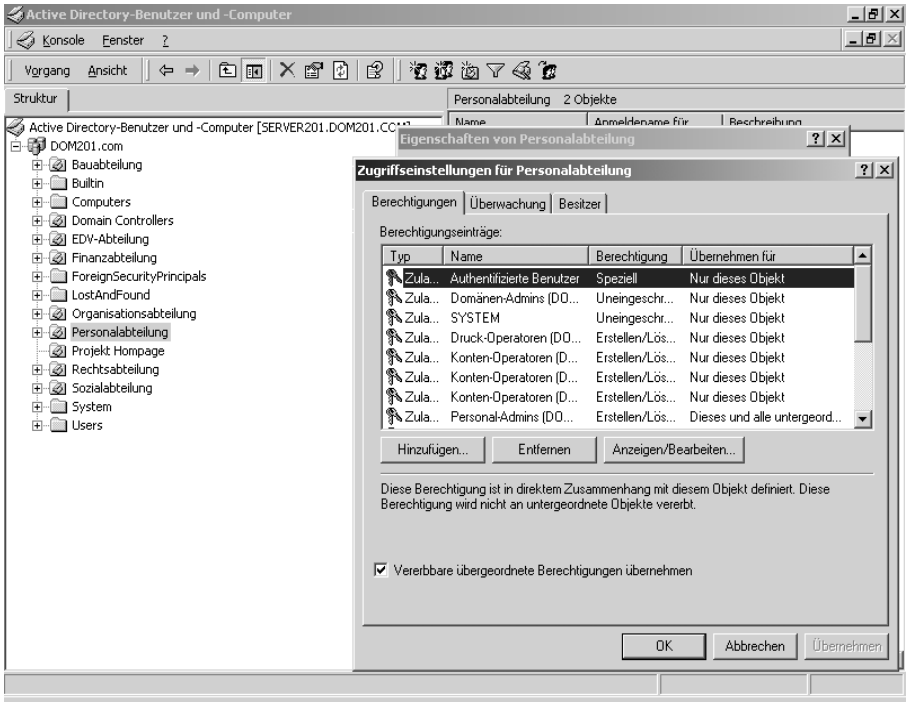
Mit dem **Assistenten** können über die Funktion *Objektverwaltung zuweisen* lediglich einige „wenige“ Berechtigungen (Aufgaben) für die Domäne oder die OE vergeben werden. Ohne Einsatz des Assistenten können hingegen auf allen Ebenen die **vollständigen** Berechtigungen über die Registerkarte *Sicherheitseinstellungen* unter *Eigenschaften* angezeigt bzw. verändert

werden. Erst in diesem Bereich wird der Umfang der Berechtigungsverwaltung deutlich. Hinzu kommt, dass die Vergabe von Berechtigungen hierarchisch nach unten vererbt wird.

5.6.1 Administrationsberechtigungen

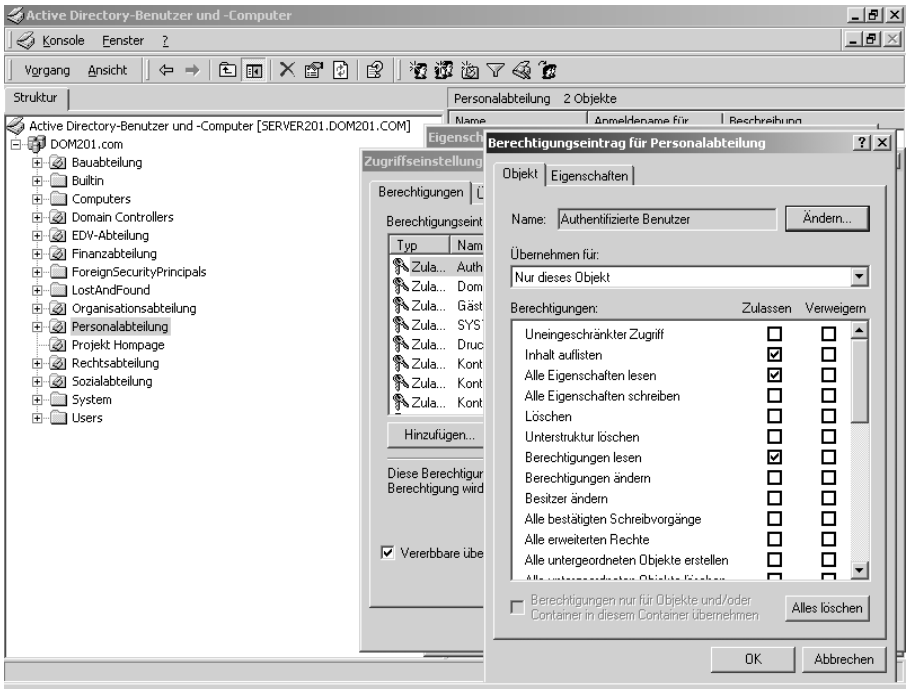
Unter der Registerkarte *Sicherheitseinstellungen* wird eine Liste der Benutzer- und Gruppenkonten angezeigt, die über einen Zugriff auf das ausgewählte Objekt verfügen. Durch Auswahl eines Benutzer- oder Gruppenkontos können dann in der Liste im unteren Teil des Fensters die am **häufigsten verwendeten** Zugriffsberechtigungen angezeigt und administriert werden. An dieser Stelle werden „**Detailberechtigungen**“ zusammengefasst und als übergeordnete **allgemeine** Berechtigungen dargestellt. Zum Beispiel verfügt die allgemeine Berechtigung *Lesen* über die Detailrechte *Inhalt lesen*, *Alle Eigenschaften lesen* und *Berechtigungen lesen*.

Je nach gewähltem Objekt können die angezeigten Rechte variieren. Grau schattierte Einträge bedeuten, dass die Berechtigungen für das entsprechende Benutzer- oder Gruppenkonto von dem übergeordneten Objekt vererbt wurden (siehe Kapitel 6). Durch die Auswahl der Schaltfläche ERWEITERT kann ein weiteres Dialogfenster aufgerufen werden, in dem **objektbezogen** eine Auflösung der Einstellungen vorgenommen werden kann.



Sicherheitseinstellungen der OE „Zugriffsberechtigungen von Personalabteilung“

Es wird angezeigt, für wen die definierten Berechtigungen gelten. Hier können weitere Einträge hinzugefügt und bestehende Einträge verändert bzw. gelöscht werden.Durch Doppelklick auf ein Benutzer- bzw. Gruppenkonto öffnet sich ein weiteres Dialogfenster, in dem alle zugewiesenen „Detailberechtigungen“ für das Objekt angezeigt werden.



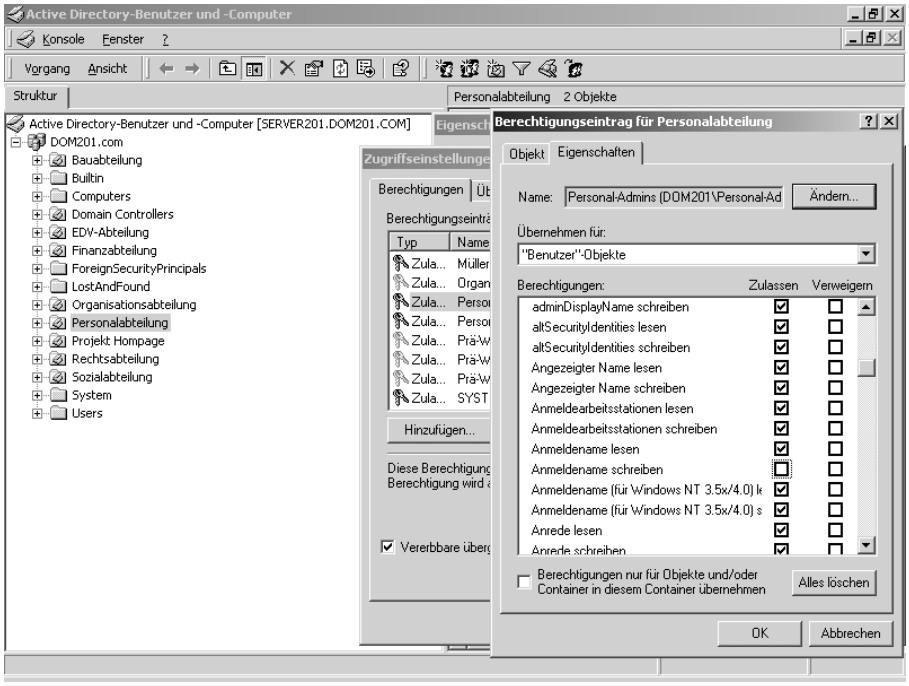
Sicherheitseinstellungen der OE „Objekt-Berechtigungen“

Die Berechtigungen unter der Registerkarte *Objekt* (siehe Abbildung oben) beziehen sich auf das Objekt (z. B. ein Benutzerkonto) insgesamt, während sich die Berechtigungen unter der Registerkarte *Eigenschaften* (siehe Abbildung nächste Seite) ausschließlich auf die Felder bzw. Attribute (z. B. Anmeldename oder Telefonnummer des Benutzerkontos) des Objektes beziehen.

- Die Verwaltung der Berechtigungen können über den *Assistenten* oder unter SICHERHEITSEINSTELLUNGEN sehr differenziert vergeben werden. Um Fehler in der Berechtigungsverwaltung zu vermeiden, sollte die Zuweisung von administrativen Aufgaben im Detail geplant und dokumentiert werden.

- Nach der Zuweisung von Berechtigungen sollten die Einstellungen unter dem entsprechenden Benutzerkonto überprüft werden.

- Die Berechtigungszuweisung kann sich auch auf Objekte des Verwaltungsprogramms *Active Directory-Standorte und -Dienste* beziehen.



Sicherheitseinstellungen der OE „Eigenschaften-Berechtigungen“

Zugriffsberechtigungen auf ein Active Directory-Objekt vergeben!

1. *Starten Sie das Verwaltungsprogramm ACTIVE DIRECTORY-BENUTZER UND -COMPUTER.*

2. *Klicken Sie im Menü ANSICHT auf ERWEITERTE FUNKTIONEN.*

3. *Klicken Sie in der Active Directory-Struktur auf ein Objekt, für das Sie die Zugriffsberechtigungen von bestimmten Eigenschaften ändern möchten. Wählen Sie in diesem Fall ein Benutzerobjekt.*

4. *Klicken Sie mit der rechten Maustaste auf den Benutzer und anschließend auf EIGENSCHAFTEN.*

5. *Wählen Sie im Fenster EIGENSCHAFTEN die Registerkarte SICHERHEITSEINSTELLUNGEN.*

6. *Klicken Sie auf der Registerkarte SICHERHEITSEINSTELLUNGEN auf ERWEITERT. Hierdurch wird das Fenster ZUGRIFFSSTEUERUNGSEINSTELLUNGEN FÜR BENUTZERNAME AUFGERUFEN.*

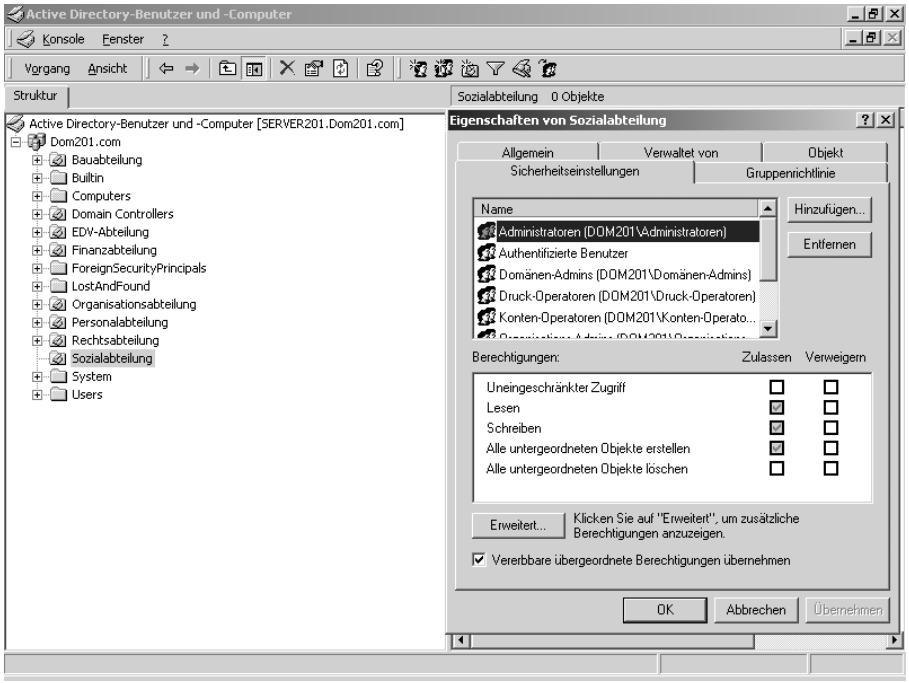
7. *In dem Fenster werden alle Berechtigungen aufgeführt, die diesem Objekt zugewiesen wurden. Wenn ein Berechtigungseintrag angezeigt wird, zu dem Sie einen Eintrag für die Zugriffssteuerung hinzufügen möchten, klicken Sie für diesen Berechtigungseintrag auf ANZEIGEN/BEARBEITEN. Klicken Sie anderenfalls auf HINZUFÜGEN, um einen neuen Berechtigungseintrag hinzuzufügen, oder auf ENTFERNEN, um eine bestehende Berechtigung zu löschen.*

8. *Durch Doppelklick auf ein Benutzer- bzw. Gruppenkonto oder durch Klicken auf ANZEIGEN/BEARBEITEN wird das Fenster BERECHTIGUNGSEINTRAG FÜR BENUTZERNAME aufgerufen. Es enthält zwei Registerkarten: OBJEKT und EIGENSCHAFTEN. Wählen Sie die Registerkarte EIGENSCHAFTEN, um die Eigenschaften für das Objekt anzuzeigen, für das Sie Zugriffsberechtigungen festlegen möchten.*

9. *Unter dieser Registerkarte können Sie festlegen, dass die Zugriffssteuerungseinträge ZULASSEN oder VERWEIGERN auf den jeweiligen Benutzer angewendet werden. Sie können beispielsweise Berechtigungen für die Felder PLZ oder TELEFON festlegen.*

5.6.2 Standardberechtigungen

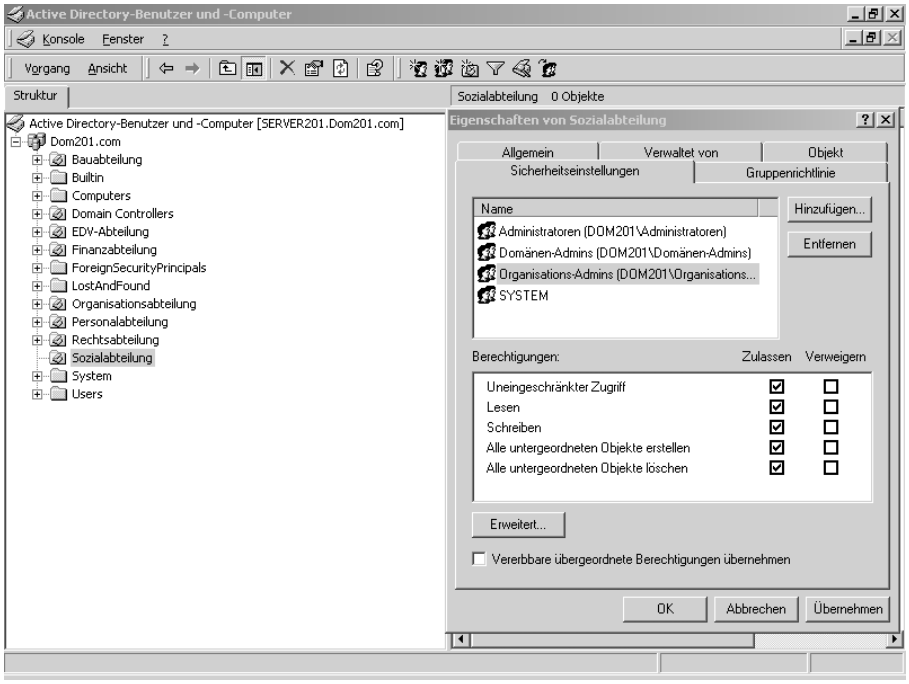
Für die Verwaltung des Active Directory ist von Windows 2000 das Gruppenkonto *Organisations-Admins* eingerichtet worden. In dieser Gruppe ist nach der Installation standardmäßig das Benutzerkonto *Administrator* Mitglied. Das Gruppenkonto verfügt über **Vollzugriffsberechtigungen** auf alle Objekte im Active Directory.



Registerkarte „Sicherheitseinstellungen auf OE-Ebene“ – Standardberechtigungen

Mit der Installation des Active Directory werden von Windows 2000 darüber hinaus **standardmäßig** auf Domänen- und Container- bzw. Organisationseinheitenebene weitere Berechtigungen an Gruppen- und Benutzerkonten vergeben. Vergleichbar ist dieses mit den Betriebssystemordnern, für die Windows 2000 ebenfalls automatisch zahlreiche NTFS-Berechtigungen vergibt.

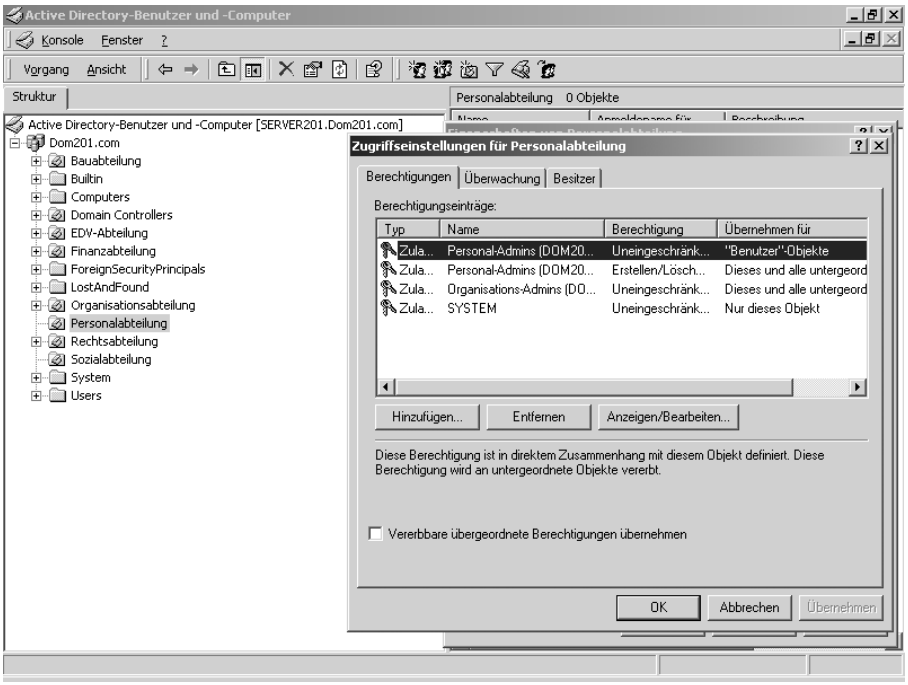
Die von Windows 2000 standardmäßig angelegte Active Directory-Struktur enthält also bereits eine Vielzahl von Berechtigungseinträgen, die auf ihre **Notwendigkeit** hin überprüft werden sollten. Da sich die Berechtigungen bei dem Hinzufügen von Objekten automatisch weitervererben, sollten die Berechtigungen auf das tatsächlich erforderliche Maß reduziert werden. Beispielsweise sind die Gruppen *Authentifizierte Benutzer*, *Jeder*, *Druck-Operatoren* und *Konten-Operatoren* zu entfernen, da sie zunächst für das Active Directory keine Bedeutung haben (siehe Kapitel 6).



Registerkarte „Sicherheitseinstellungen auf OE-Ebene“ – Erforderliche Berechtigungen

Im Active Directory sollte in Bezug auf die Administrationsbefugnisse der **Grundsatz** gelten: „Es werden nur so viele Berechtigungen vergeben, wie administrativ notwendig sind.“ Beachten Sie aber, dass dem Administrator bei der Zuweisung von Freigabe- und NTFS-Berechtigungen nur die Benutzer- und Gruppenkonten angezeigt werden, für die er im Active Directory Administrationsrechte erhalten hat.

Sofern die Administration des Active Directory nicht delegiert wird, sollte ausschließlich das Gruppenkonto *Organisations-Admins* über Befugnisse im Active Directory verfügen. Zusätzliche Gruppenkonten können dann hinzugefügt werden, wenn die Administration des Active Directory auf mehrere Administratoren verteilt wird oder einzelne Administratoren besondere Aufgaben, wie z. B. die Benutzerkontenverwaltung, übernehmen.



Registerkarte „Sicherheitseinstellungen auf OE-Ebene“ – Delegierte Berechtigungen

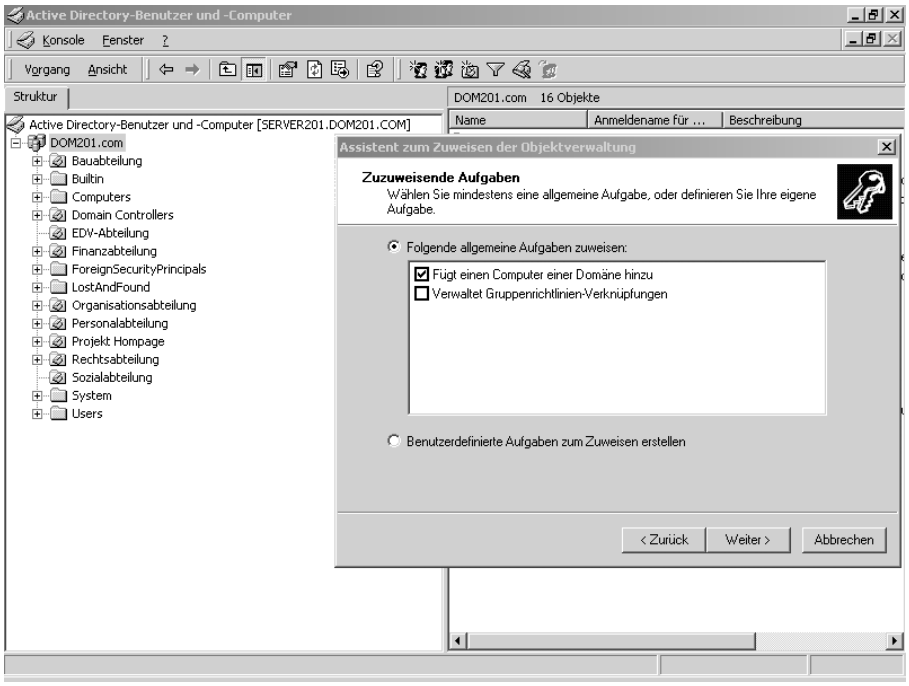
Sie sollten auf keinen Fall auf der **Domänenebene** die Gruppe *Organisations-Admins* entfernen. Das würde dazu führen, dass Sie sich als Administrator die Berechtigung für das Active Directory entziehen und somit **aussperren**. Sie haben weder über das Verwaltungsprogramm noch über die Wiederherstellungskonsole die Möglichkeit, die Berechtigungen wiederherzustellen. Sie könnten nur über die Datensicherungsbänder die Datenbank des Active Directory zurücksichern. Sollten keine Datensicherungsbänder mit der Active Directory-Datenbank vorliegen, müssen Sie den Domänencontroller herabstufen, um anschließend das Active Directory neu zu installieren. Das hätte einen Verlust aller Objekte (Benutzerkonten, Computerkonten, Organisationseinheiten usw.) und Berechtigungszuweisungen zur Folge.

5.6.3 Assistent für die Rechteverwaltung

Auf der Domänenebene können einem Benutzer- oder Gruppenkonto über den **Assistenten** folgende „allgemeine“ Aufgaben in Form von Berechtigungen zugewiesen werden:

- **Fügt einen Computer einer Domäne hinzu:** Nachdem diese „Aufgabe“ z. B. dem neu angelegten Gruppenkonto *Help-Desk-Admins* zugewiesen wurde, können die Administratoren dieser Gruppe einen Computer in die Domäne aufnehmen.

- **Verwaltet Gruppenrichtlinien-Verknüpfungen:** Mithilfe dieser „Aufgabe“ können vorhandene Gruppenrichtlinien Objekten (z. B. Organisationseinheiten) zugeordnet werden.



Objektverwaltung zuweisen auf Domänenebene, „Zuzuweisende Aufgaben“

Wenn hingegen auf der Ebene der Organisationseinheiten (OE) der Assistent aufgerufen wird, können einem Benutzer- oder Gruppenkonto bzw. einem Administrator folgende „Aufgaben“ zugewiesen werden:

- **Erstellt, entfernt und verwaltet Benutzerkonten**: Es können ausschließlich Benutzerkonten innerhalb der OE verwaltet werden. Die Befugnisse Setzt Kennwörter von Benutzerkonten zurück und Liest alle Benutzerinformationen sind enthalten.

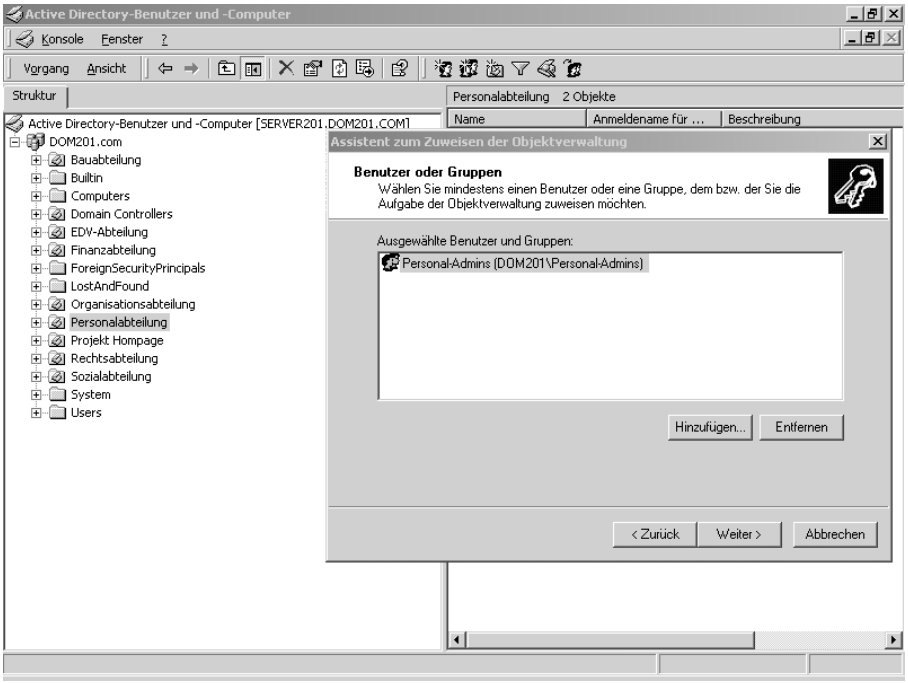
- **Setzt Kennwörter von Benutzerkonten zurück**: Es können Kennwörter der innerhalb einer OE angelegten Benutzerkonten zurückgesetzt werden.

- **Liest alle Benutzerinformationen**: Die Benutzerkonten können mit lesendem Zugriff aufgerufen werden.

- **Erstellt, entfernt und verwaltet Gruppen**: Die Administration wird auf die Verwaltung von Gruppenkonten beschränkt.

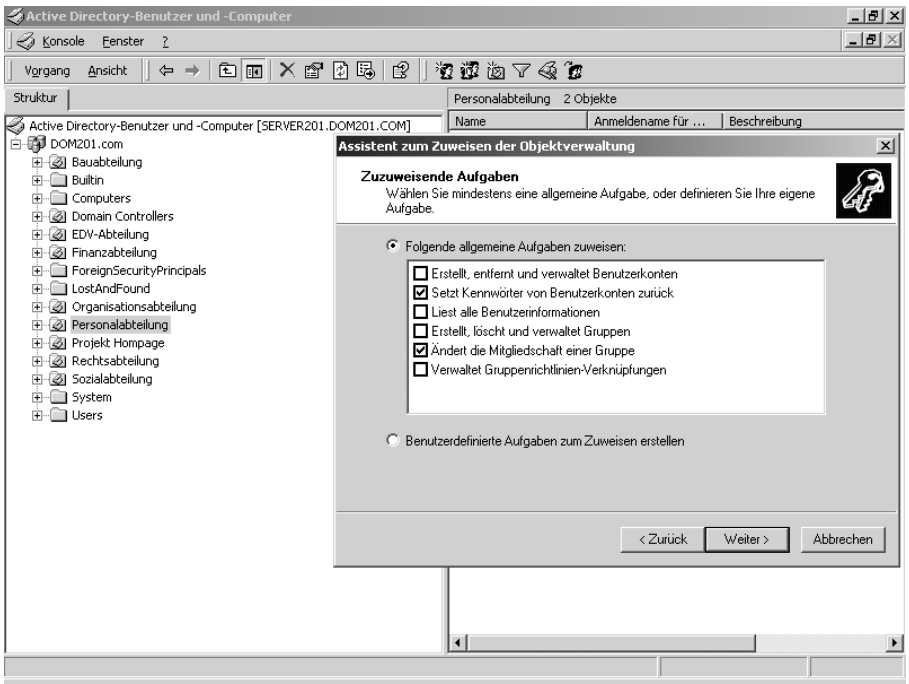
- **Ändert die Mitgliedschaft einer Gruppe**: Es können ausschließlich die Mitgliedschaften verwaltet werden.

- **Verwaltet Gruppenrichtlinien-Verknüpfungen**: Der Organisationseinheit können Gruppenrichtlinien zugeordnet werden.

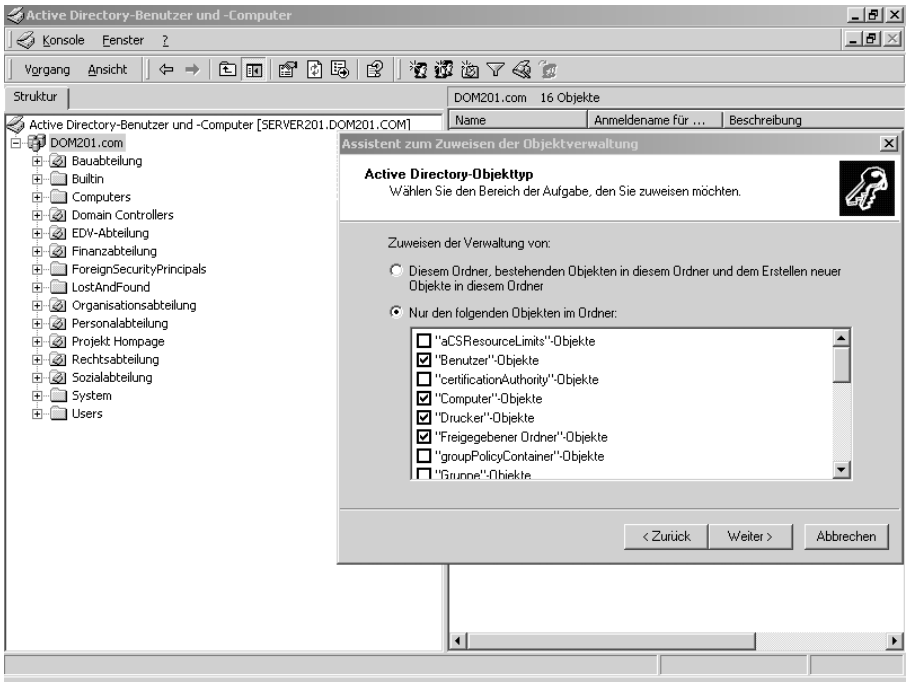


Objektverwaltung zuweisen auf OE-Ebene, Benutzer und Gruppen hinzufügen

Über die Schaltfläche BENUTZERDEFINIERTE AUFGABEN ZUM ZUWEISEN ERSTELLEN können alternativ **spezifische Objektberechtigungen** vergeben werden

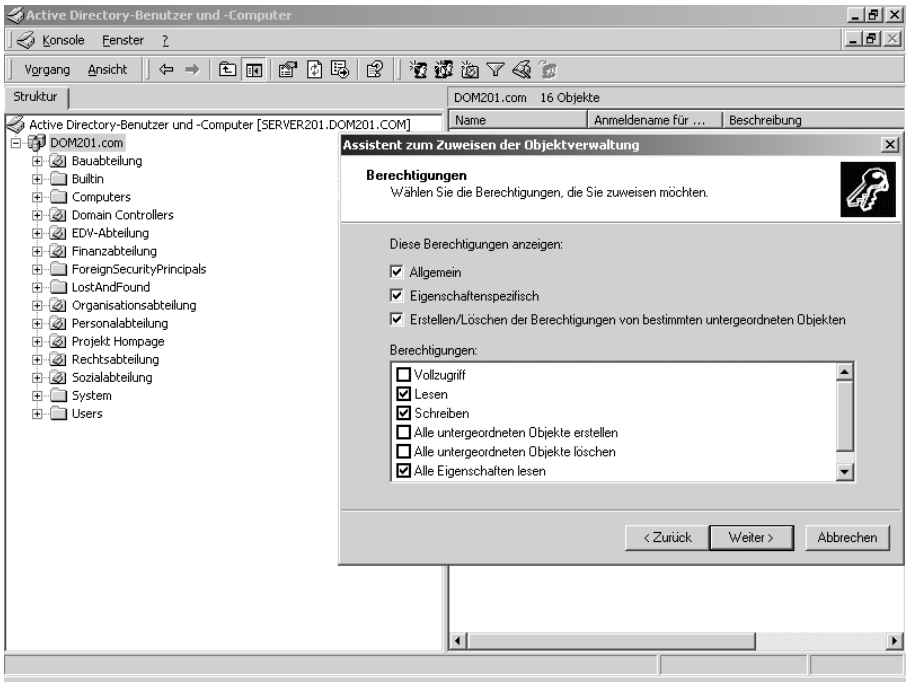


Objektverwaltung zuweisen auf OE-Ebene, „Zuzuweisende Aufgaben“



Objektverwaltung zuweisen, „Active Directory-Objekttyp“

Nachdem ein oder mehrere Objekte ausgewählt wurden, können im nächsten Schritt die Berechtigungen gesetzt werden. Es stehen drei Optionen zum **Anzeigen der Berechtigungen** zur Auswahl:



Objektverwaltung zuweisen, „Berechtigungen“

- **Allgemein**: Es stehen für alle Objekte gleichermaßen anwendbare Berechtigungen, wie z. B. Lesen und Schreiben usw., zur Auswahl. Die Berechtigungen beziehen sich auf das gesamte Objekt, d. h., auch die Eingabefelder bzw. Eigenschaften eines Objektes erhalten diese Berechtigungen.

- **Eigenschaftenspezifisch**: Mit dieser Option können die Berechtigungen Lesen und Schreiben für Eigenschaften bzw. Eingabefelder eines Objektes vergeben werden. Der Assistent zeigt jedoch nur einige Eigenschaften der einzelnen Objekte z. T. in abgekürzter englischer Sprache an. Vollständig können die Eigenschaften von Objekten über die Registerkarte Sicherheitseinstellungen administriert werden.

  Das Objekt Benutzerkonto verfügt z. B. über zahlreiche Eingabefelder (Anrede, Anmeldename usw.) für die jeweils lesende und/oder schreibende Befugnisse vergeben werden können. Soll beispielsweise das Eingabefeld Anmeldename eines Benutzerkontos vor administrativen Veränderungen geschützt werden, ist dem entsprechenden Benutzerkonto die Schreibberechtigung für dieses Eingabefeld zu entziehen.

- **Erstellen/Löschen der Berechtigungen von bestimmten untergeordneten Objekten**: Die Option ermöglicht es, Berechtigungen zu vergeben, um weitere Objekte innerhalb einer OE zu erstellen und/oder zu löschen.

Die Berechtigungen stehen also in **Abhängigkeit** zu den einzelnen Objekten, d. h., es werden nur die Berechtigungen angezeigt, die für das ausgewählte Objekt verwendbar sind. Mit der Festlegung der Berechtigungen ist die Arbeit mit dem Assistenten abgeschlossen. Im letzten Fenster des Assistenten können die vorgenommenen Einstellungen noch einmal überprüft werden.

- Mit dem Assistenten können im Active Directory keine Berechtigungen entzogen bzw. verändert werden.

- Berücksichtigen Sie, dass mit der Erstellung einer Organisationseinheit (OE) von Windows 2000 automatisch Berechtigungen der OE zugewiesen werden. Nach Abschluss der Berechtigungszuweisung über den **Assistenten** sollten Sie diese über die Registerkarte SICHERHEITSEINSTELLUNGEN kontrollieren und ggf. nicht erforderliche Berechtigungen entfernen.

Mithilfe des Assistenten einem Benutzerkonto die Objektverwaltung auf der OE-Ebene zuweisen!

1. *Klicken Sie auf START-PROGRAMME-VERWALTUNG und wählen Sie ACTIVE DIRECTORY-BENUTZER UND -COMPUTER.*
2. *Klicken Sie mit der rechten Maustaste auf die OE, für die Sie die Rechte delegieren möchten.*
3. *Wählen Sie OBJEKTVERWALTUNG ZUWEISEN, um den ASSISTENTEN ZUM ZUWEISEN DER OBJEKTVERWALTUNG zu starten.*
4. *Klicken Sie in dem Fenster WILLKOMMEN auf WEITER.*
5. *Klicken Sie auf die Schaltfläche HINZUFÜGEN, um Benutzer- oder Gruppenkonten auszuwählen, auf die die Objektverwaltung delegiert werden soll.*
6. *Wählen Sie im Feld SUCHEN IN die Domäne aus, in der die Benutzer- oder Gruppenkonten verwaltet werden.*
7. *Wählen Sie aus der Liste die Benutzer- oder Gruppenkonten aus und klicken Sie anschließend auf die Schaltfläche HINZUFÜGEN. Klicken Sie auf OK. Falls Sie weitere Benutzer oder Gruppen hinzufügen möchten, klicken Sie erneut auf die Schaltfläche HINZUFÜGEN und wiederholen das beschriebene Verfahren, bis Sie alle gewünschten Benutzer und Gruppen hinzugefügt haben.*
8. *Klicken Sie auf WEITER und aktivieren Sie die Kontrollkästchen für die Aufgaben, die Sie delegieren möchten. Falls die entsprechende Aufgabe in der Liste nicht aufgeführt wird, können Sie auf BENUTZERDEFINIERTE AUFGABEN ZUM ZUWEISEN ERSTELLEN klicken.*
9. *Klicken Sie auf WEITER. Der Assistent fasst jetzt die von Ihnen gewählten Optionen zusammen. Falls alle Optionen korrekt sind, klicken Sie auf die Schaltfläche FERTIGSTELLEN, um Ihre Änderungen zu übernehmen.*

5.7 Active Directory-Administration unter Windows 2000 Professional

Die Administration des Active Directory ist sehr vielfältig und kann in der Regel nur an der Konsole des Domänencontrollers durchgeführt werden. Um die Arbeit des Administrators zu erleichtern und administrative Aufgaben des Active Directory auf Arbeitsplätze einzelner Administratoren zu verlagern, kann der Zugriff auf die Verwaltungsprogramme des Active Directory auf einem Computer unter Windows 2000 Professional eingerichtet werden. Die **Windows 2000-Verwaltungsprogramme** ermöglichen die **Remoteverwaltung** eines Servers bzw. eines Domänencontrollers von einem beliebigen Computer unter Windows 2000.

Die Windows 2000-Verwaltungsprogramme werden auf dem Client durch die Datei adminpak.msi installiert. Bereits nach der Installation können Verwaltungsaufgaben im Active Directory durchgeführt werden.

Wenn Sie die Windows 2000-Verwaltungsprogramme installieren und ausführen möchten, müssen Sie über Administratorrechte für den betreffenden Computer verfügen. Sie benötigen außerdem Administratorrechte für die Domäne, in der Sie Verwaltungsaufgaben für die Remoteverwaltung des Servers ausführen möchten.

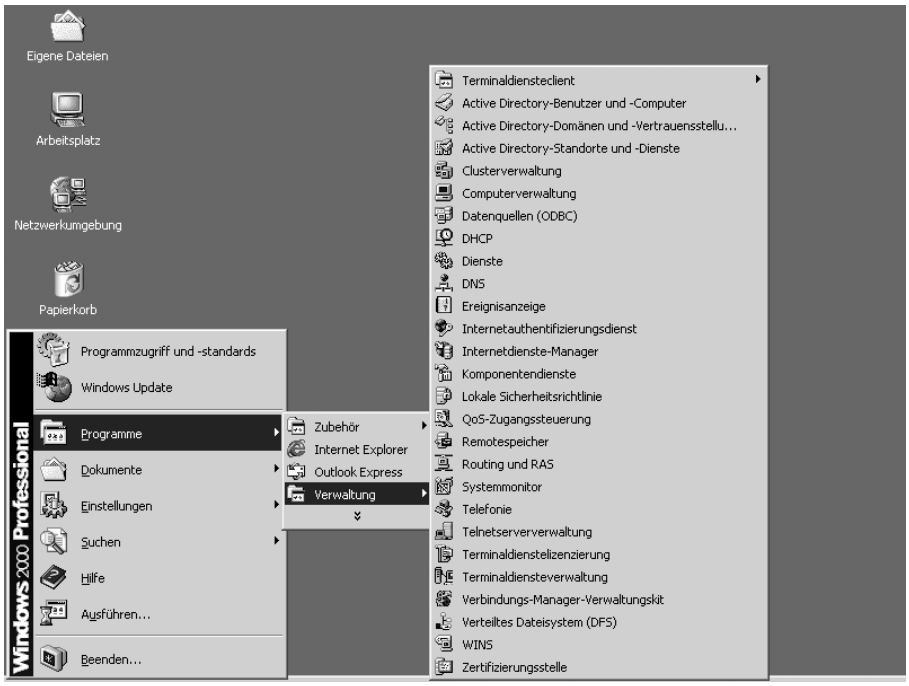
Windows 2000-Verwaltungsprogramme auf einem Client installieren!

1. *Öffnen Sie auf der entsprechenden Windows 2000 Server-CD den Ordner I386. Die aktuelle Version der Windows 2000-Verwaltungsprogramme befindet sich auf der Windows 2000 Service Pack-CD.*
2. *Doppelklicken Sie auf die Datei adminpak.msi.*
3. *Klicken Sie auf WEITER und dann auf FERTIGSTELLEN.*
4. *Mit der Datei adminpak.msi werden die Active Directory-Verwaltungsprogramme sowie andere Verwaltungsprogramme installiert.*

Die Verwendung der Windows 2000-Verwaltungsprogramme für die Remoteausführung von Verwaltungsaufgaben auf einem Domänencontroller ist natürlich nur dann möglich, wenn der Computer über ein **Computerkonto** in der Domäne verfügt.

Computerkonto in der Domäne erstellen!

1. *Starten Sie in der Systemsteuerung SYSTEM.*
2. *Klicken Sie auf der Registerkarte NETZWERKIDENTIFIKATION auf EIGENSCHAFTEN.*
3. *Klicken Sie unter MITGLIED VON auf DOMÄNE. Geben Sie den Namen der gewünschten Domäne ein und klicken Sie dann auf OK.*
4. *Sie werden aufgefordert, einen Benutzernamen und ein Benutzerkennwort einzugeben, um den Computer in die Domäne einzubinden.*
5. *Klicken Sie auf OK, um das Dialogfeld SYSTEMEIGENSCHAFTEN zu schließen.*
6. *Sie werden aufgefordert, den Computer neu zu starten, um die Änderungen zu übernehmen.*



Windows 2000 Server-Verwaltungsprogramme auf dem Client

Verwenden der Windows 2000 Server-Verwaltungsprogramme!

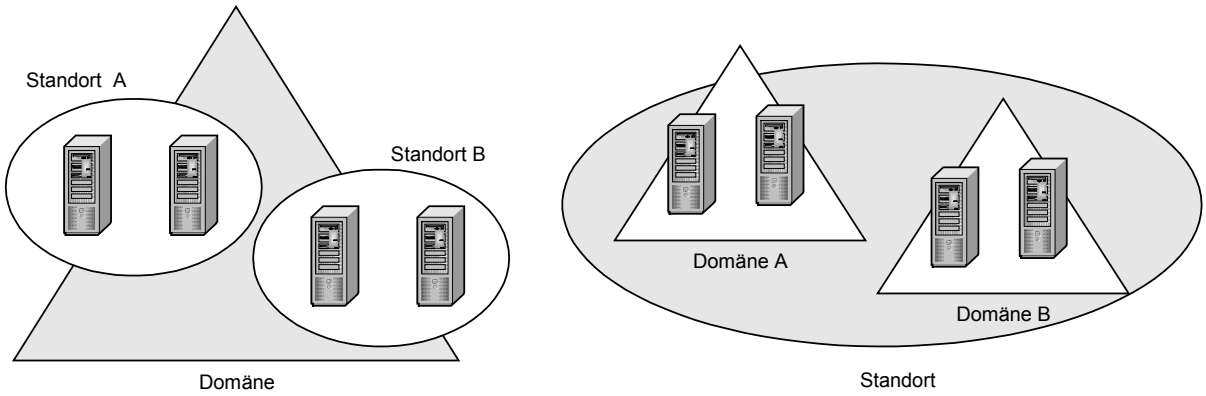
1. *Melden Sie sich an der Windows 2000 Professional-Arbeitsstation unter dem Benutzerkonto des Domänenadministrators an.*
2. *Klicken Sie auf START, zeigen Sie auf PROGRAMME, anschließend auf VERWALTUNG.*
3. *Klicken Sie dann auf eines der enthaltenen Server-Verwaltungsprogramme.*

5.8 Standort (Site)

Ein weiteres Element in der Architektur des Active Directory ist der Standort (Site). Während Domänen bzw. Domänengesamtstrukturen eher eine **logische** Darstellungsform für die im Netzwerk vorhandenen Ressourcen sind, gehen Standorte auf die **physikalische** Struktur des Netzwerkes ein. Ein Standort umfasst dabei Computer, die in einem Netzwerk physikalisch gruppiert wurden. Mehrere solcher Standorte lassen sich über eine entsprechende Standortverbindung (Site Link) miteinander verbinden.

Zwischen der physikalischen Struktur eines Netzwerkes und der Gesamtstruktur von Domänen muss keine entsprechende Beziehung bestehen. Analog verhält es sich mit Standorten und

dem Domänennamensraum eines Active Directory. Ein einziger Standort kann beispielsweise mehrere Domänen umfassen. Ebenso wäre es möglich, dass sich eine Domäne über mehrere Standorte hinweg ausdehnt.



Logische und physikalische Struktur (Domänen und Standorte)

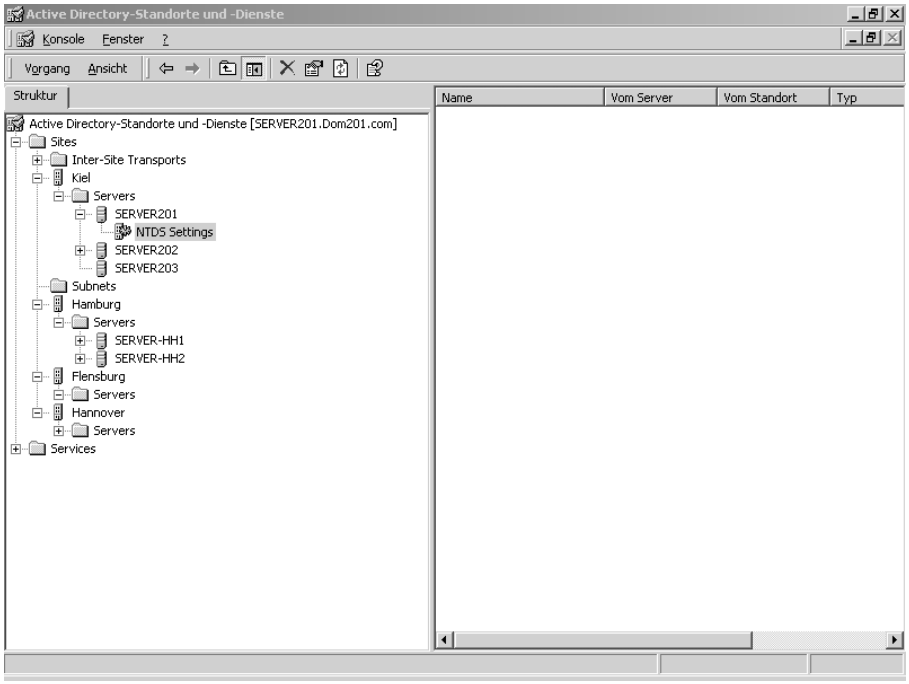
Bei der Installation des Active Directory wird der erste Standort *Standardname-des-ersten-Standorts* automatisch erstellt. Ein Standort besteht aus **Server-Objekten** und sollte über mindestens einen Domänencontroller verfügen. Bestehen mehrere Standorte, so sind Verknüpfungen zwischen den Standorten für die **Replikation** herzustellen.

Standorte vereinfachen folgende Aufgaben:

- **Authentifizierung:** Bei der Anmeldung eines Clients über ein Domänenkonto sucht die Anmelderoutine zuerst nach einem Domänencontroller, der sich im selben Standort wie der Client befindet. Da zunächst versucht wird, auf Domänencontroller am Standort des Clients zuzugreifen, bleibt der Netzwerkverkehr auf diesen Standort beschränkt.

- **Replikation:** Active Directory-Informationen werden sowohl innerhalb als auch zwischen Standorten repliziert. Das Active Directory repliziert Daten innerhalb eines Standortes häufiger als zwischen Standorten. Diese Vorgehensweise schafft einen Ausgleich zwischen der Nachfrage nach möglichst aktuellen Verzeichnisinformationen und den durch die verfügbare Netzwerkbandbreite vorgegebenen Beschränkungen.

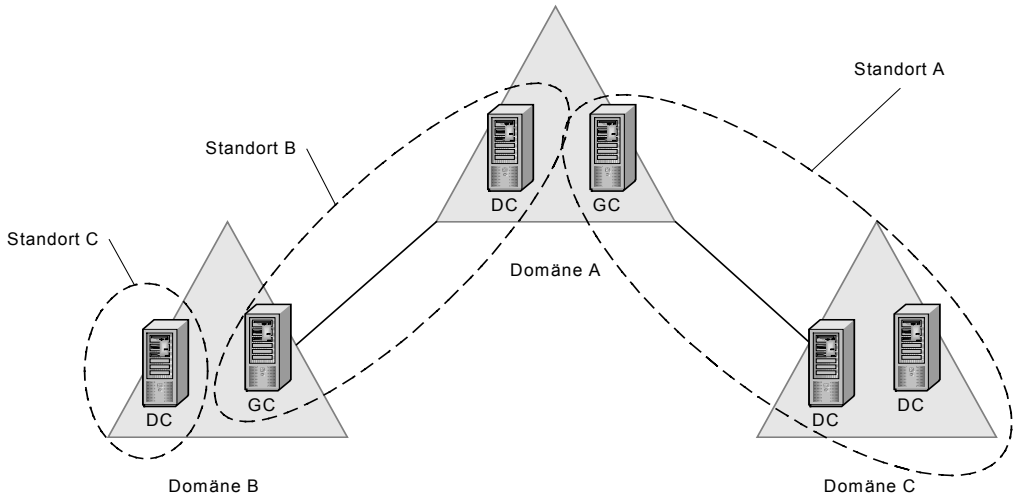
- **Dienste mit Active Directory-Unterstützung:** Mithilfe von Standorten kann die Verteilung von Dienstinformationen leichter strukturiert und optimiert werden. Die aktuellen Informationen sind folglich für Clients verfügbar und können im gesamten Netzwerk bereitgestellt werden.



Active Directory-Standorte und -Dienste

5.9 Replikation

Die Replikation von **Änderungen** der Active Directory-Informationen spielt dann eine Rolle, wenn **mehrere** Domänencontroller in einem Windows 2000-Netzwerk installiert sind. Jeder Domänencontroller repliziert bzw. **synchronisiert** seine Active Directory-Datenbank mit anderen Domänencontrollern in der Domänengesamtstruktur. Die Bedeutung der Replikation von Active Directory-Informationen steigt mit der Größe des Netzwerkes.



Replikation

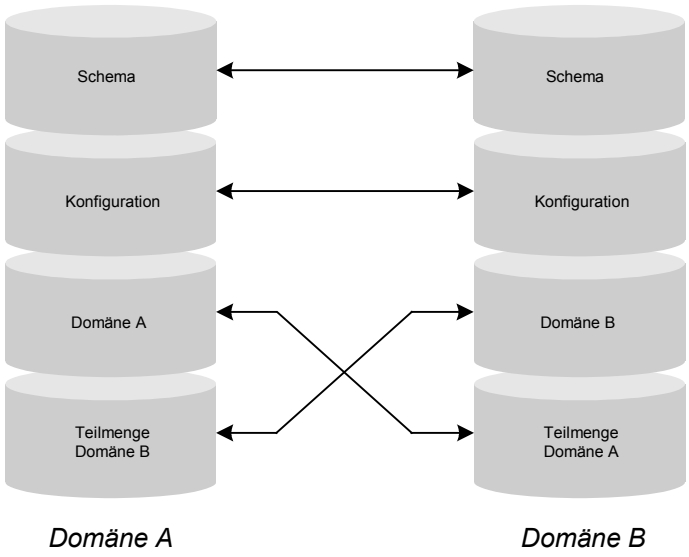
Die Active Directory-Datenbank ist in mehrere **Verzeichnispartitionen** eingeteilt, die jede für sich eine eigene **Replikationsmethode** bzw. Topologie aufweist:

- **Schemapartition:** Sie enthält die Definition und Beschreibung der Objekte und Attribute. Die Schemapartition ist eine so genannte Organisationspartition. Sie wird in der Domänengesamtstruktur auf alle Domänencontroller repliziert, damit jedes Objekt nach den gleichen Regeln erstellt und bearbeitet werden kann.

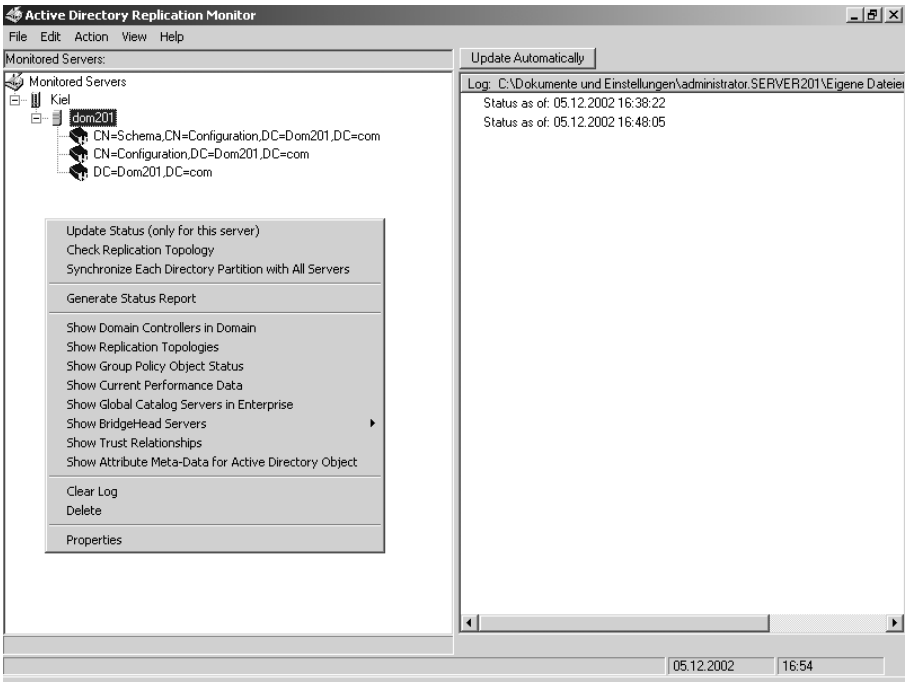
- **Konfigurationspartition:** Sie enthält Informationen über die Struktur von Active Directory und beinhaltet Angaben über die vorhandenen Domänen und Standorte. Existierende Domänencontroller und die angebotenen Dienste sind ihr bekannt. Sie wird deshalb ebenfalls als Organisationspartition auf alle Domänencontroller in der Domänengesamtstruktur repliziert.

- **Domänenpartition:** Sie enthält die domänenspezifischen Informationen und speichert die Objekte einer Domäne, wie z. B. Benutzer, Computer, Gruppen und Organisationseinheiten. Sie wird nur auf die Domänencontroller der entsprechenden Domäne repliziert.

- **Partielle Domänen-Verzeichnispartition (globaler Katalog-Server):** Ein globaler Katalog-Server enthält außer den drei oben genannten Verzeichnispartitionen eine zusätzliche partielle Domänen-Verzeichnispartition, die die Teilmenge aller in der Domänengesamtstruktur enthaltenen Objekte enthält.



Verzeichnisreplikation von Globalen Katalog-Servern zwischen Domänen



Active Directory-Replikationsmonitor (Support-Tools)

Die Replikation kann über das Verwaltungsprogramm *Active Directory-Standorte und -Dienste* gesteuert werden. Darüber hinaus ist in den **Support-Tools** ein *Active Directory-Replikationsmonitor* für Abfragen und Auswertungen enthalten.

Er verfügt z. B. über folgende wichtige Funktionen:

- Abfragen aktueller Statistiken und des Replikationsstatus des Servers,
- Durchführen der Synchronisation und
- Anzeige der Replikationstopologie der Domänencontroller.

5.10 Sicherheitscheck

- *Vor der **Installation** des Active Directory sollten Sie Folgendes festlegen:*
  - *DNS-Namensraum,*
  - *Speicherort der Datenbank,*
  - *Struktur des Active Directory,*
  - *Aufgaben- bzw. Berechtigungszuweisungen in Bezug auf die Administration,*
  - *Datensicherung bzw. Replikation des Active Directory.*

- *Sie sollten die Datenbank des Active Directory in größeren Netzwerken auf **separaten Datenträgern** verwalten.*
- *Das Anlegen von Organisationseinheiten (OE) **vereinfacht** die Administration. Sie bilden die Grundlage für die Abgrenzung von Administrationsbefugnissen und die Zuweisung von Gruppenrichtlinien.*
- *Prüfen Sie die Administrationsbefugnisse im Active Directory sorgfältig und begrenzen Sie sie auf ein **Minimum**. Der Assistent vereinfacht die Zuweisung von administrativen Aufgaben.*
- *Die Gruppe **Organisations-Admins** hat die Aufgabe, das Active Directory zu verwalten. Sie verfügt über **Vollzugriffsrechte** auf allen Ebenen und darf auf der Domänenebene **nicht** entfernt werden.*
- *Nach der Installation der Datei adminpak.msi können Sie das Active Directory von einem **Windows 2000 Professional Client** administrieren.*
- *In **größeren** Netzwerken sollten Sie zur besseren Auslastung des Netzwerkverkehrs STANDORTE einrichten.*
- *Um eine hohe Verfügbarkeit (Replikation) des Active Directory zu gewährleisten, sollten Sie innerhalb jeder Domäne **zwei Domänencontroller** einrichten.*

6 Benutzer- und Gruppenverwaltung

In diesem Kapitel erfahren Sie,

- was bei dem Anlegen von Benutzer- und Gruppenkonten zu beachten ist,
- den Unterschied zwischen lokalen Benutzerkonten, Domänenbenutzer- und Gruppenkonten,
- welche Bedeutung die von Windows 2000 standardmäßig erstellten Benutzer- und Gruppenkonten haben,
- über welche Eigenschaften die Benutzer- und Gruppenkonten verfügen und
- welche Richtlinien und Strategien bei der Benutzer- und Gruppenkontenverwaltung berücksichtigt werden sollten.

6.1 Planung der Benutzer- und Gruppenkonten

Eine **gründliche** Verwaltung der Benutzer- und Gruppenkonten ist entscheidend für die **ordnungsgemäße** Zuweisung von Zugriffsberechtigungen. Rechte autorisieren einen Benutzer zum Ausführen bestimmter Aktionen auf einem Computer, wie z. B. das Ausführen einer Fachanwendung oder das Sichern von Dateien und Ordnern eines Computers. Eine Berechtigung ist eine einem Objekt (normalerweise einer Datei, einem Ordner oder einem Drucker) zugewiesene Regel, die festlegt, welche Benutzer- bzw. Gruppenkonten auf welche Weise Zugriff auf das Objekt haben.

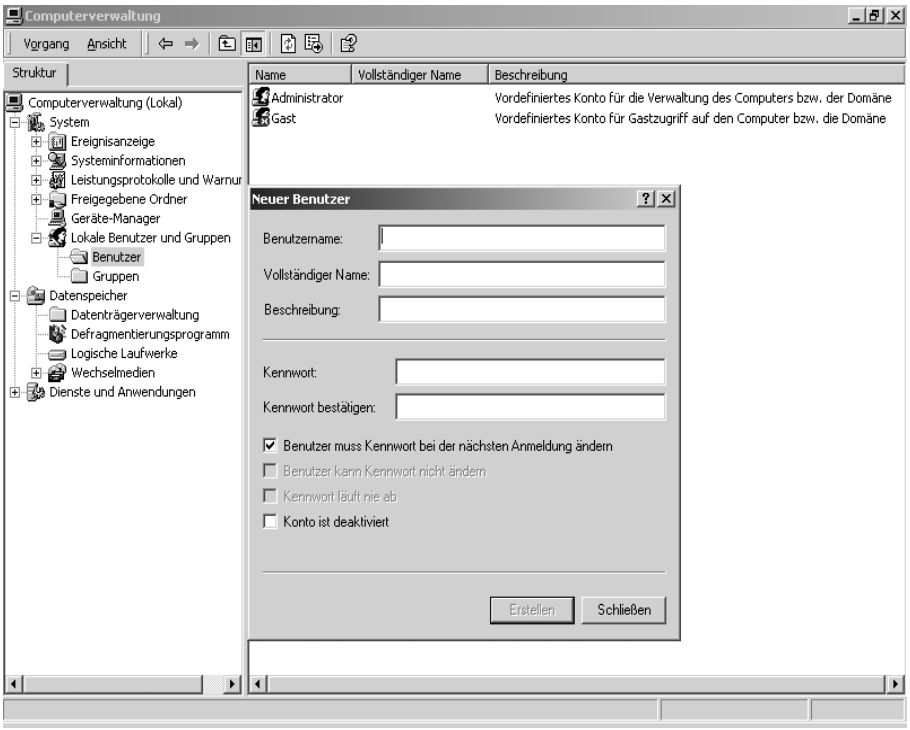
Die Verwaltung der Benutzer- und Gruppenkonten sollte wie folgt geplant werden:

- *Planen Sie, welche Gruppen Sie für Ihre Organisationsstruktur benötigen und welche Benutzerkonten welchen Gruppen zugeordnet werden sollen.*
- *Berücksichtigen Sie, dass für die Benutzerauthentifizierung Kennwortrichtlinien eingesetzt werden sollten.*
- *Es ist festzulegen, inwieweit die Computernutzung auf* ANMELDEZEITEN *und* ANMELDUNGEN AN AUSGEWÄHLTEN COMPUTERN *eingeschränkt werden soll.*

Auch Windows 2000 verfügt über keine **Reportfunktion**, die z. B. die Verwaltung der Benutzer- und Gruppenkonten sowie die ihnen zugewiesenen Zugriffsberechtigungen hinreichend transparent machen. Sie sollten deshalb sehr **strukturiert** und **systematisch** die Objekte im Active Directory administrieren. Für die Nachvollziehbarkeit einiger Einstellungen können Sie das Tool *DumpSec* einsetzen (siehe Kapitel 11).

6.2 Lokale Benutzer- und Gruppenkonten

Lokale Benutzerkonten ermöglichen einem Benutzer, sich nur an dem Computer anzumelden, auf dem ein lokales Benutzerkonto erstellt wurde. Es können dann nur die Ressourcen des betreffenden Computers genutzt werden. Die lokalen Benutzer- und Gruppenkonten sind **nicht** Bestandteil des Active Directory und werden deshalb mit dem Verwaltungsprogramm *Computerverwaltung* erstellt.



Computerverwaltung – Lokale Benutzer und Gruppen, Neuer Benutzer

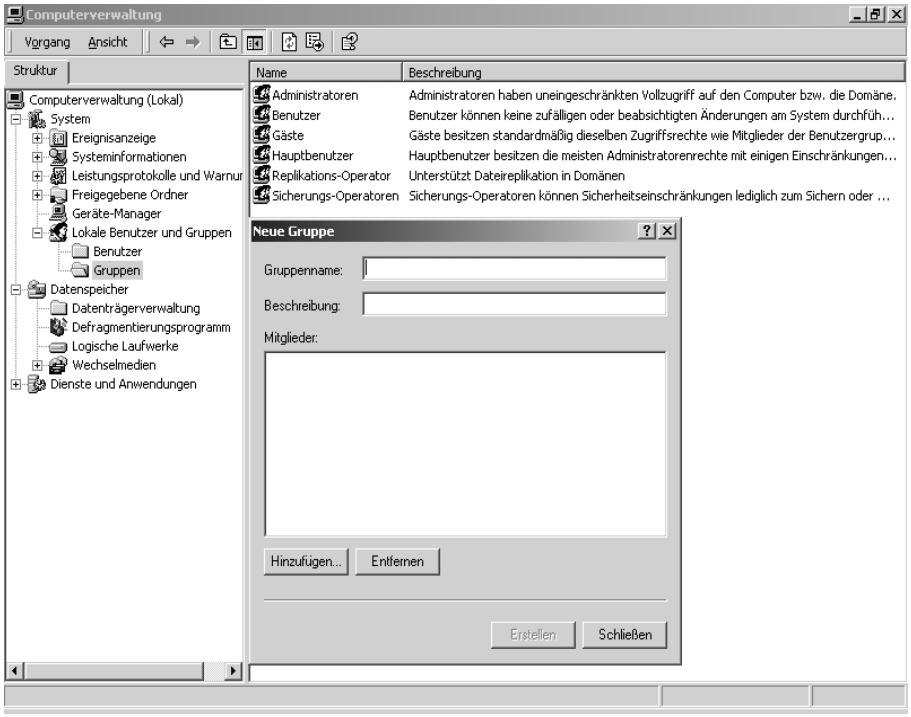
Windows 2000 erstellt automatisch die vordefinierten Benutzerkonten *Administrator* und *Gast*. Diese Konten können nicht gelöscht werden.

Da das vordefinierte Benutzerkonto *Administrator* allgemein bekannt ist und nicht deaktiviert werden kann, sollten Sie es umbenennen. Im Gegensatz zu Windows NT 4.0 ist das Gastkonto unter Windows 2000 standardmäßig deaktiviert.

Die Informationen für die **Authentifizierung** werden, wie unter Windows NT 4.0, in der Datei *SAM* (Security Account Manager) im Ordner <*Winnt**system32**config*> gespeichert. Mit der Installation von Windows 2000 werden diese Informationen zusätzlich in dem Ordner <*Winnt**system32**repair*> gesichert. Benutzer- und Gruppenkonten, die im **Active Directory** angelegt werden, werden nicht in der SAM-Datei, sondern in der Active Directory-Datenbank verwaltet. Für lokale Benutzer- und Gruppenkonten können ausschließlich die **lokalen Sicherheitsrichtlinien** berücksichtigt werden.

Die mit dem Betriebssystem Windows 2000 Professional ausgestatteten Computer verfügen über die folgenden vordefinierten lokalen Gruppen:

Lokale Gruppe	**Beschreibung**
Benutzer	Benutzerkonten werden automatisch Mitglied dieser Gruppe. Administrative Befugnisse sind weitgehend unterbunden.
Administratoren	Mitglieder können alle Verwaltungsaufgaben auf dem Computer ausführen. Das Benutzerkonto *Administrator* ist standardmäßig Mitglied dieser Gruppe.
Gäste	Das Benutzerkonto *Gast* ist Mitglied dieser Gruppe. Mitglieder können nur eingeschränkt die Funktionen von Windows nutzen. Sie können nicht dauerhaft die Desktop-Umgebung ändern.
Sicherungs-operatoren	Mitglieder dieser Gruppe können mit *Windows Backup* ausschließlich die Dateien des Computers sichern und wiederherstellen.
Hauptbenutzer	Mitglieder dieser Gruppe verfügen über weitgehende Administrationsrechte, wie z. B. Benutzerkonten erstellen und/oder Ressourcen freigeben.
Replikations-operatoren	Mitglieder können Datenreplikationsdienste konfigurieren.



Computerverwaltung – Lokale Benutzer und Gruppen, Neue Gruppe

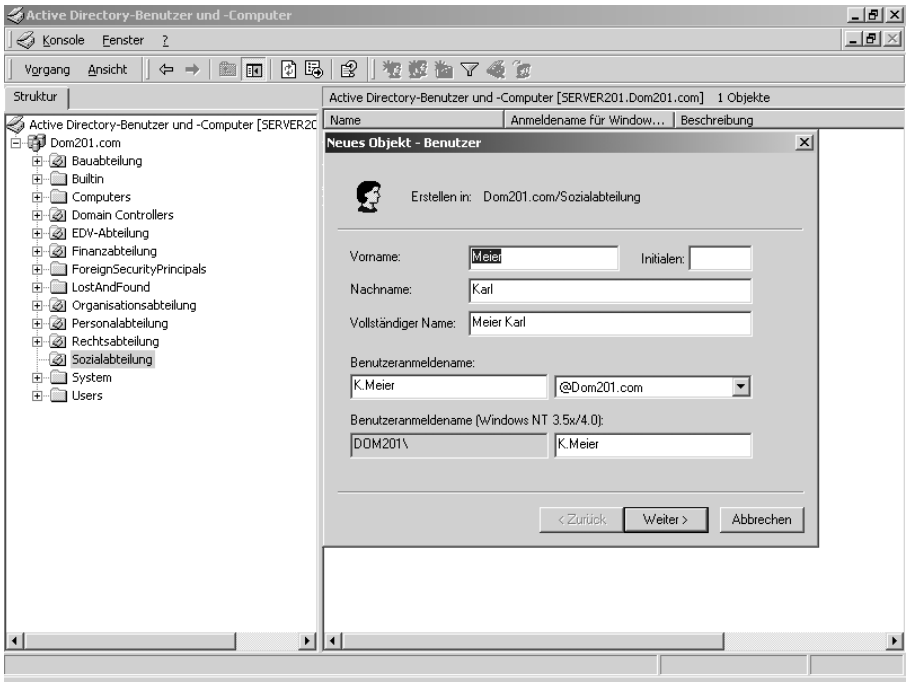
6.3 Domänen-Benutzerkonten verwalten

Domänen-Benutzerkonten ermöglichen einem Benutzer, sich an einer Domäne anzumelden und auf Netzwerkressourcen zuzugreifen. Die Domänen-Benutzerkonten werden auf einem **Domänencontroller** über das Verwaltungsprogramm *Active Directory-Benutzer und -Computer* erstellt.

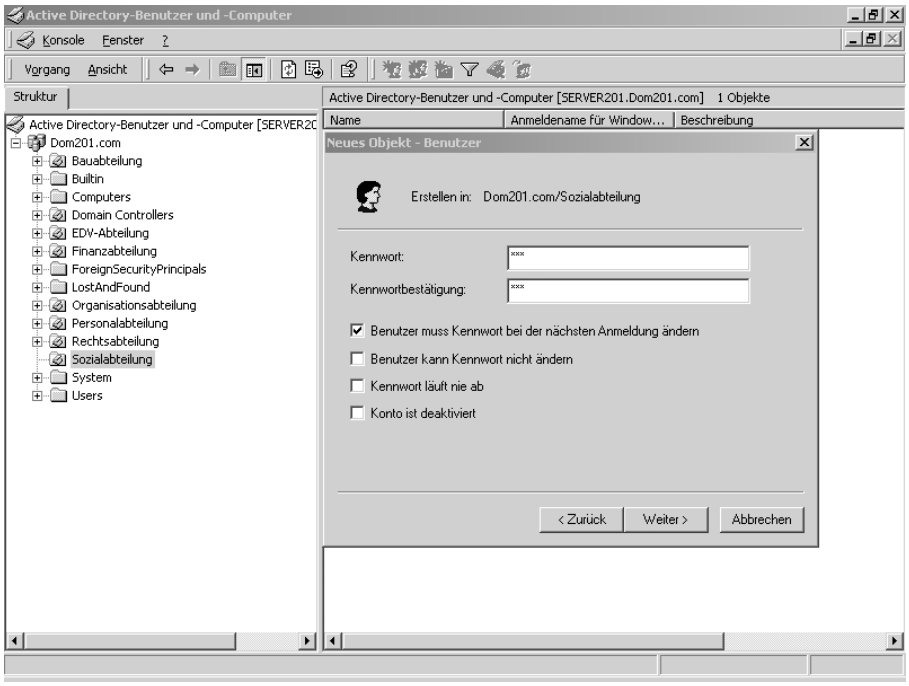
Benutzerkonto anlegen!

1. *Rufen Sie ACTIVE DIRECTORY-BENUTZER UND -COMPUTER auf.*
2. *Klicken Sie mit der rechten Maustaste auf die Organisationseinheit, in der das neue Konto erstellt werden soll.*
3. *Zeigen Sie auf NEU und wählen Sie BENUTZER.*
4. *In dem Dialogfenster geben Sie den vollständigen Namen und den Benutzeranmeldenamen ein.*
5. *Klicken Sie auf WEITER, um in einem weiteren Dialogfenster die Kennworteinstellungen zu erfassen.*

Mit der Installation des Active Directory werden das Administrator- und das Gast-Benutzerkonto eingerichtet. Das Gast-Benutzerkonto ist standardmäßig deaktiviert. Beide Benutzerkonten werden neben den von Windows 2000 installierten Gruppenkonten im Container *Users* aufgeführt (siehe Tz. 6.4).



Benutzerkonto anlegen - Stammdaten



Benutzerkonto anlegen - Kennworteinstellungen

- Beachten Sie, dass die Daten im Datenfeld VOLLSTÄNDIGER NAME im Active Directory angezeigt werden. Geben Sie deshalb eindeutige Namen ein.
- Benutzernamen dürfen aus bis zu 20 Zeichen bestehen. Groß- und Kleinschreibung wird unterschieden. Folgende Zeichen dürfen nicht enthalten sein: „ / \ [ ] : ; | = , + * ? < >. Leerzeichen und Punkte können verwendet werden, aber ein Benutzername kann nicht ausschließlich aus diesen Zeichen bestehen.
- Das Kontrollkästchen BENUTZER MUSS KENNWORT BEI DER NÄCHSTEN ANMELDUNG ÄNDERN sollte aktiviert werden, damit der Benutzer vom System aufgefordert wird, ein eigenes, nur ihm bekanntes Kennwort zu wählen.
- Benennen Sie das Benutzerkonto *Administrator* um. Es verfügt über Vollzugriffsrechte in allen Bereichen. Legen Sie für jeden Administrator ein eigenständiges Konto an.

Neues Kennwort durch den Administrator vorgeben!

1. *Klicken Sie mit der rechten Maustaste auf das Benutzerkonto des entsprechenden Benutzers.*
2. *Zeigen Sie auf KENNWORT ZURÜCKSETZEN.*
3. *Geben Sie ein neues Kennwort ein und aktivieren Sie das Kontrollkästchen BENUTZER MUSS DAS KENNWORT BEI DER NÄCHSTEN ANMELDUNG ÄNDERN.*

Authentifizierung

Die Authentifizierung ist ein wesentlicher Aspekt der Systemsicherheit. Sie bestätigt die Identität jedes Benutzers, der versucht, sich an einer Domäne anzumelden oder auf Netzwerkressourcen zuzugreifen. Außerdem wird anhand der Windows 2000-Authentifizierung die einmalige Anmeldung für sämtliche Netzwerkressourcen ermöglicht. Mit einer einmaligen Anmeldung an der Domäne kann sich ein Benutzer mit einem Kennwort bzw. einer Smartcard auf jedem Computer innerhalb dieser Domäne authentifizieren.

Authentifizierungsprozess

Die erfolgreiche Benutzeranmeldung in einer Windows 2000-Umgebung findet in zwei getrennten Phasen statt: Durch die *interaktive Anmeldung* wird die Identität des Benutzers für ein Domänen- oder ein lokales Benutzerkonto geprüft, während bei der *Netzwerkauthentifizierung* die Identität des Benutzers für sämtliche in Anspruch genommenen Netzwerkdienste bestätigt wird.

Authentifizierungstypen

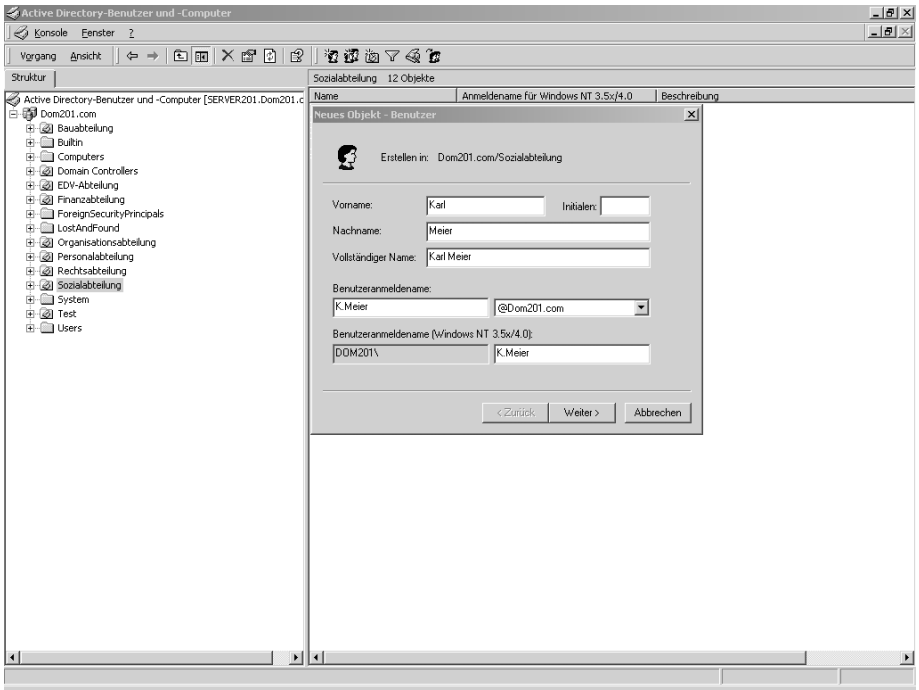
Bei der Authentifizierung eines Benutzers verwendet Windows 2000 folgende Authentifizierungsarten:

Die **Kerberos-Authentifizierung** wird zur Authentifizierung von Windows 2000-Benutzern eingesetzt (siehe Kapitel 10).

Die **NTLM-Authentifizierung** wird verwendet, wenn der Client oder Server mit einer früheren Version von Windows arbeitet.

Ein Standardvorgang bei der Anmeldung eines Benutzers besteht darin, die Identität des Benutzers festzustellen. Die Identität wird bestätigt, wenn der Benutzer das richtige Kennwort für sein Benutzerkonto eingibt. Wenn z. B. ein Benutzer versucht, eine Serververbindung herzustellen, um auf eine Datei zuzugreifen, muss der Server sicher sein, dass es sich tatsächlich um diesen Benutzer handelt. Bei einer NTLM-Authentifizierung geht der Server davon aus, dass es sich um den Benutzer handelt, der das richtige Kennwort zu seinem Benutzerkonto eingibt.

Eine höhere Sicherheit wird bei der Verwendung der Kerberos-Authentifizierung erreicht. Sie enthält einen Dienst, der als eine vertrauenswürdige Stelle die Identität des Benutzers überprüft und für die Zeit einer Client/Server-Sitzung so genannte Tickets ausstellt. Das Ticket enthält u. a. einen Sitzungsschlüssel, den Namen des Benutzers, für den der Sitzungsschlüssel ausgestellt wurde, sowie die Ablaufzeit des Tickets. Da der Server dem Kerberos-Dienst bei der Überprüfung der Benutzeridentität vertraut, akzeptiert der Server das Ticket als Beweis der Authentizität des Benutzers.



Eigenschaften des Benutzerkontos – Registerkarte Allgemein

Nach dem Anlegen eines Benutzerkontos können ihm weitere **Eigenschaften** über *Registerkarten* zugeordnet werden (die Option ANSICHT-ERWEITERTE FUNKTIONEN muss aktiviert sein, damit alle Registerkarten angezeigt werden):

Bearbeiten der Eigenschaften!

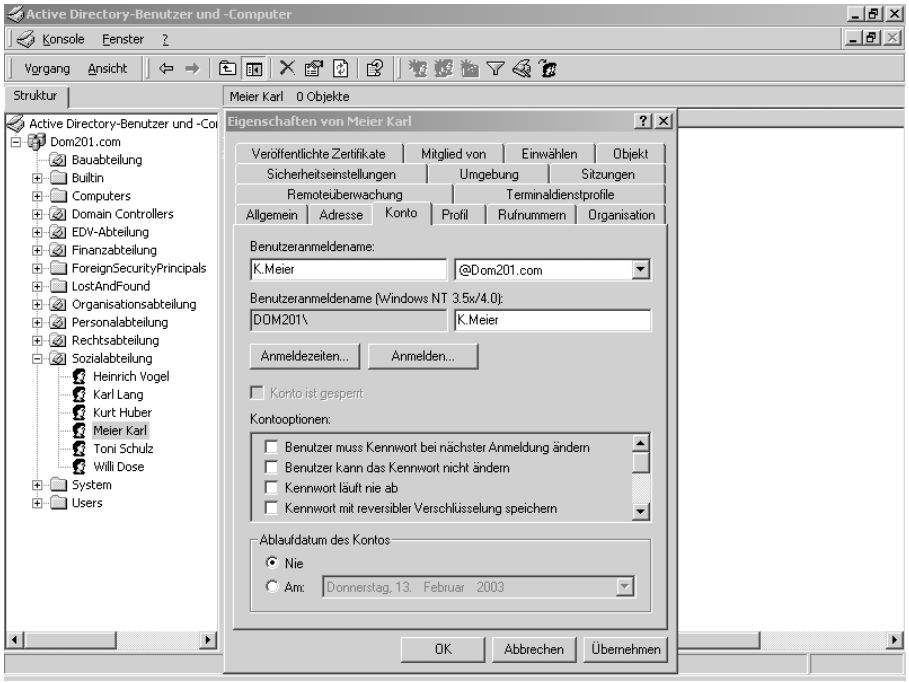
1. *Wählen Sie mit der linken Maustaste ein Benutzerkonto aus.*
2. *Sobald Sie auf die rechte Maustaste drücken, öffnet sich ein Menüfenster.*
3. *Zeigen Sie auf EIGENSCHAFTEN und bestätigen Sie mit der linken Maustaste.*
4. *Es öffnet sich ein Eigenschaftenfenster mit der aktiven Registerkarte ALLGEMEIN.*
5. *Klicken Sie auf die Registerkarte, deren Eigenschaften Sie bearbeiten möchten.*

Registerkarten für persönliche Eigenschaften

Zu den Registerkarten für persönliche Einstellungen zählen *Allgemein*, *Adresse*, *Rufnummern* und *Organisation*. Durch das Ausfüllen der Felder können Benutzer präziser zugeordnet und über die Active Directory-Suchfunktionen schneller aufgefunden werden.

Registerkarte *Konto*

Funktion	**Beschreibung**
Anmeldename	Die Änderung des Anmeldenamens ist möglich.
Anmeldezeiten	Der Benutzer kann am Client nur innerhalb der festgelegten Anmeldezeiten arbeiten.
Anmelden an	Der Benutzer kann sich nur an bestimmten Clients anmelden.
Kontosperrung	Der Administrator kann hier die Kontosperrung aufheben, sofern das Benutzerkonto durch die mehrmalige Falscheingabe des Kennwortes gesperrt wurde.
Kontooptionen	Es können Optionen für die Behandlung des Kennwortes festgelegt werden.
Ablaufdatum des Kontos	Das Benutzerkonto wird nach Eingabe eines definierbaren Ablaufdatums bei dessen Erreichen automatisch gesperrt.



Eigenschaften des Benutzerkontos – Registerkarte Konto

Verwechseln Sie die Kontosperrung nicht mit der Kontodeaktivierung. Die Kontosperrung wird durch die Falscheingabe des Kennwortes (bei aktiven Kennwortrichtlinien) automatisch aktiviert, während der Administrator ein Benutzerkonto jederzeit deaktivieren kann, indem er mit der rechten Maustaste auf ein Benutzerkonto klickt und im Menü die Option KONTO DEAKTIVIEREN ausführt.

Registerkarte *Profil*

Auf der Registerkarte *Profil* wird der Pfad zu der Netzwerkfreigabe angegeben, in der servergespeicherte Profile gespeichert werden (siehe Kapitel 7). Darüber hinaus kann ein Anmeldeskript für die Ausführung bestimmter Befehle oder Anwendungen unmittelbar nach der Anmeldung angegeben und ein Basisordner bzw. ein so genanntes Homeverzeichnis für die Ablage von Dateien voreingestellt werden.

Registerkarte *Veröffentlichte Zertifikate*

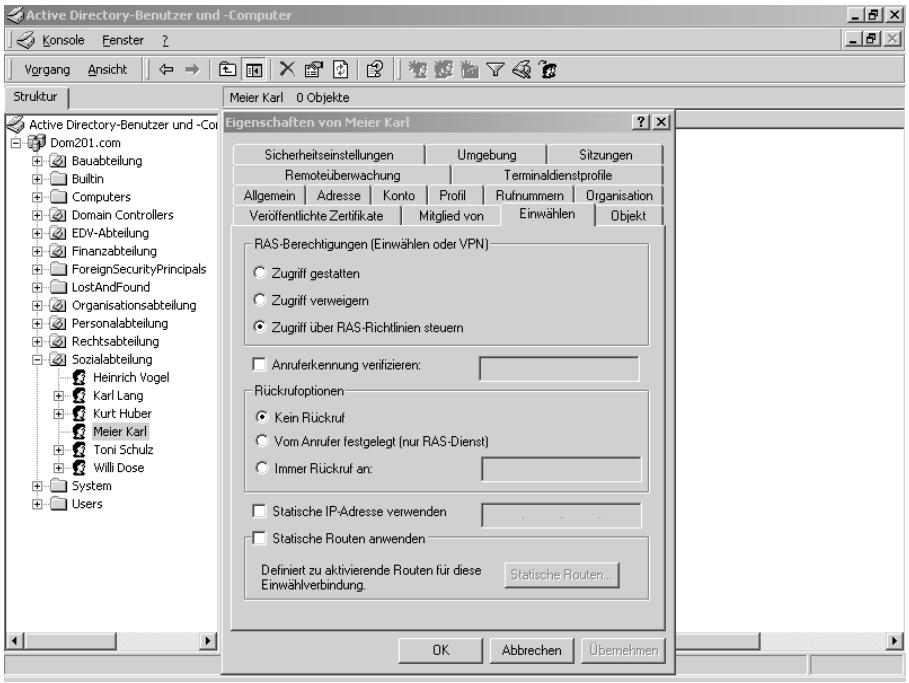
Ein Zertifikat bezeichnet eine Datensammlung, die zur Authentifizierung eingesetzt wird und den sicheren Austausch von Informationen in nicht gesicherten Netzwerken (Internet) gewährleistet. Ein Zertifikat bindet einen öffentlichen Verschlüsselungsschlüssel an die Einheit, die den entsprechenden privaten Verschlüsselungsschlüssel enthält. Dem Benutzerkonto können über diese Registerkarte Zertifikate zugeordnet werden.

Registerkarte *Mitglied von*

Gruppen werden eingesetzt, um Verwaltungsaufgaben zu vereinfachen. Alle Benutzerkonten, die einer Gruppe zugeordnet werden, erhalten automatisch die Befugnisse, die der entsprechenden Gruppe zugewiesen wurden. Wird eine Gruppe unter dieser Registerkarte entfernt, ist das Benutzerkonto nicht mehr Mitglied dieser Gruppe.

Registerkarte *Einwählen*

Mit der Registerkarte *Einwählen* kann gesteuert werden, wie Benutzer von einem Remotecomputer – einem Computer außerhalb des internen Netzwerkes – eine DFÜ-Verbindung mit dem internen Netzwerk herstellen können.



Eigenschaften des Benutzerkontos – Registerkarte Einwählen

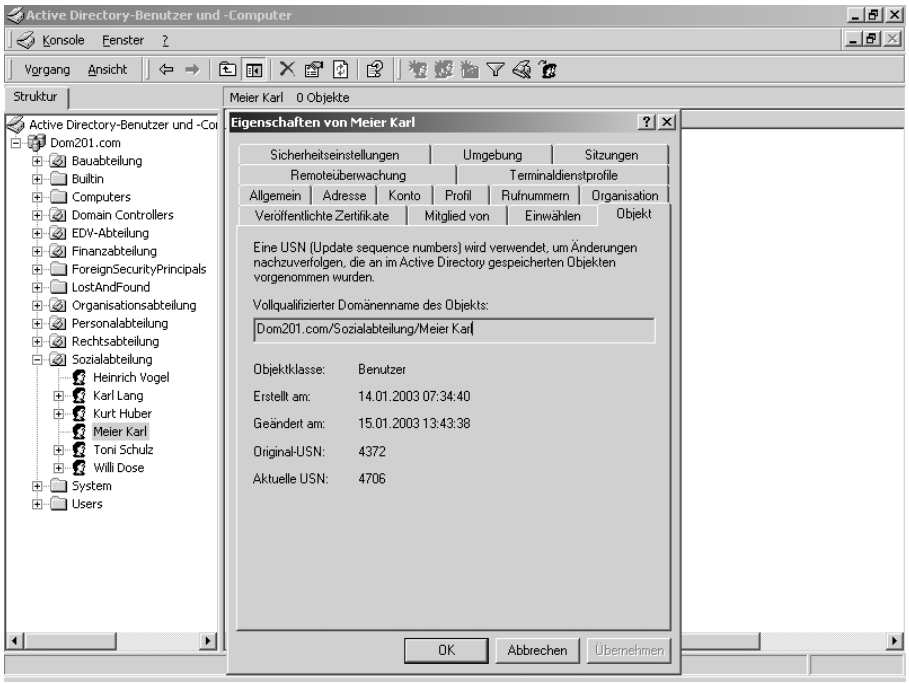
- Es ist zu empfehlen, grundsätzlich die Option IMMER RÜCKRUF AN zu aktivieren, um bei einer Einwahl in das interne Netz einen automatischen Rückruf einzuleiten.

- Neben den Einstellungen auf der Registerkarte EINWÄHLEN müssen Sie die Installation und Konfiguration eines RAS-Servers berücksichtigen. Des Weiteren sind entsprechende Hardwarekomponenten für den Anschluss ans Telefonnetz notwendig. Nur unter diesen Voraussetzungen ist eine Einwahl möglich.

- Berücksichtigen Sie, dass fernadministrative Aktivitäten nur dann möglich sein sollten, wenn sie von Ihnen eingeleitet und überwacht werden können. Zugänge externer Dienstleister sind nach Abschluss der Administration sofort wieder zu deaktivieren.

Registerkarte Objekt

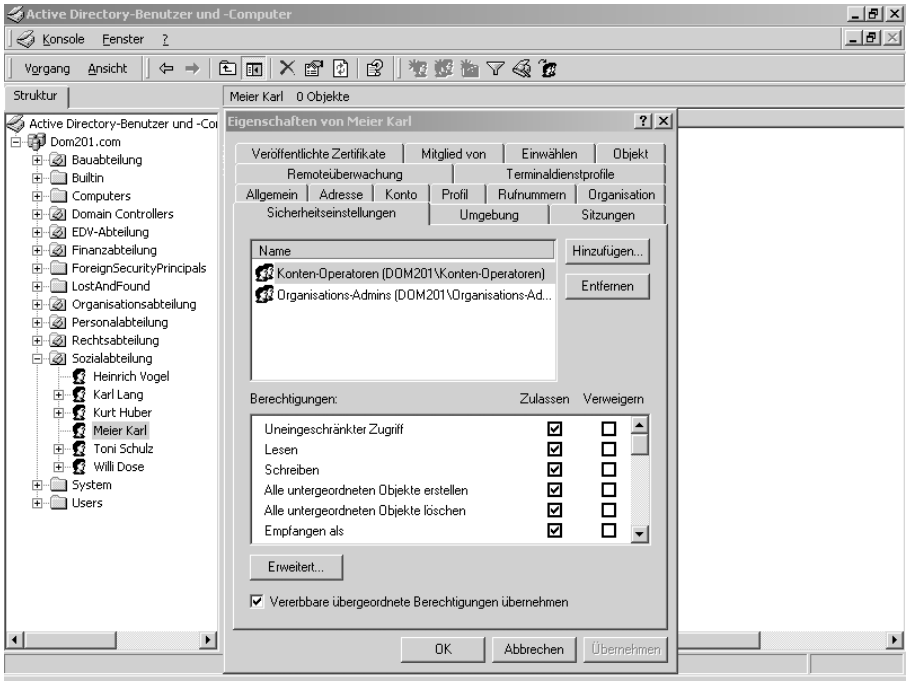
Die Registerkarte *Objekt* liefert den voll qualifizierten Domänennamen des Objekts. Darüber hinaus enthält sie zusätzliche Informationen, z. B. die Objektklasse, das Erstellungs- und Änderungsdatum, die Original-USN (Unique Sequence Number) sowie die aktuelle USN. USN werden verwendet, um Änderungen von Objekten im Active Directory zu verfolgen. Die Daten auf der Registerkarte sind nicht administrierbar.



Eigenschaften des Benutzerkontos – Registerkarte Objekt

Registerkarte Sicherheitseinstellungen

Mithilfe der Registerkarte *Sicherheitseinstellungen* können Berechtigungen für die Administration dieses Objektes (Benutzerkonto) vergeben werden. Soll beispielsweise erreicht werden, dass nur ein bestimmter Administrator oder eine speziell angelegte Administratorengruppe Benutzerkonten verwaltet, können die entsprechenden Berechtigungen über diese Registerkarte vergeben werden (siehe Kapitel 5).



Eigenschaften des Benutzerkontos – Registerkarte Sicherheitseinstellungen

- Sicherheitseinstellungen bzw. Berechtigungen für die Administration von Active Directory-Objekten sollten Sie nach Möglichkeit auf der Ebene der Organisationseinheiten vergeben.

- Beachten Sie, dass eine differenzierte Vergabe von Berechtigungen für jedes einzelne Objekt die Nachvollziehbarkeit der zugewiesenen Befugnisse erheblich erschwert.

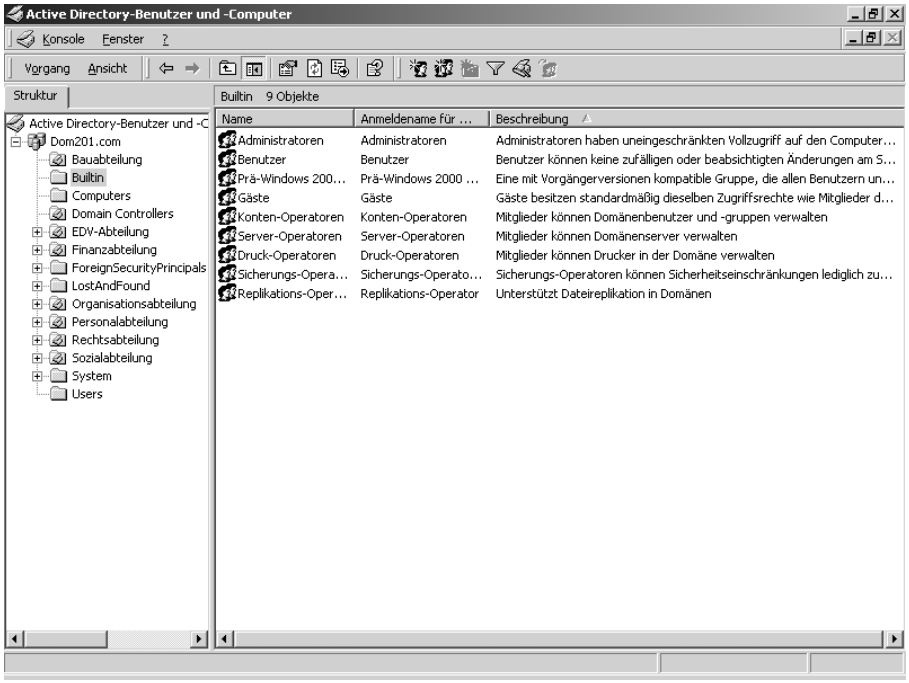
- Berücksichtigen Sie, dass die Gruppe *Organisations-Admins* immer über Vollzugriffsrechte verfügt. Dieser Gruppe ist standardmäßig das Benutzerkonto *Administrator* zugeordnet.

Registerkarten für Terminaldienste

Die Registerkarten für Terminaldienste umfassen die Registerkarten *Umgebung*, *Sitzungen*, *Remoteüberwachung* und *Terminaldienstprofile*. Die Terminaldienste ermöglichen Benutzern, sich über eine **Terminalemulation** bzw. von einem Terminal (Thin-Client) anzumelden, um Windows 2000 nutzen zu können. Zu den Informationen auf den Registerkarten für Terminaldienste zählen beispielsweise der Zeitpunkt und die Beendigung einer Anmeldung sowie die Speichermethode für bestimmte Desktop-Einstellungen.

6.4 Standard-Domänen-Benutzer- und Gruppenkonten

6.4.1 Die Gruppenkonten im Container Builtin



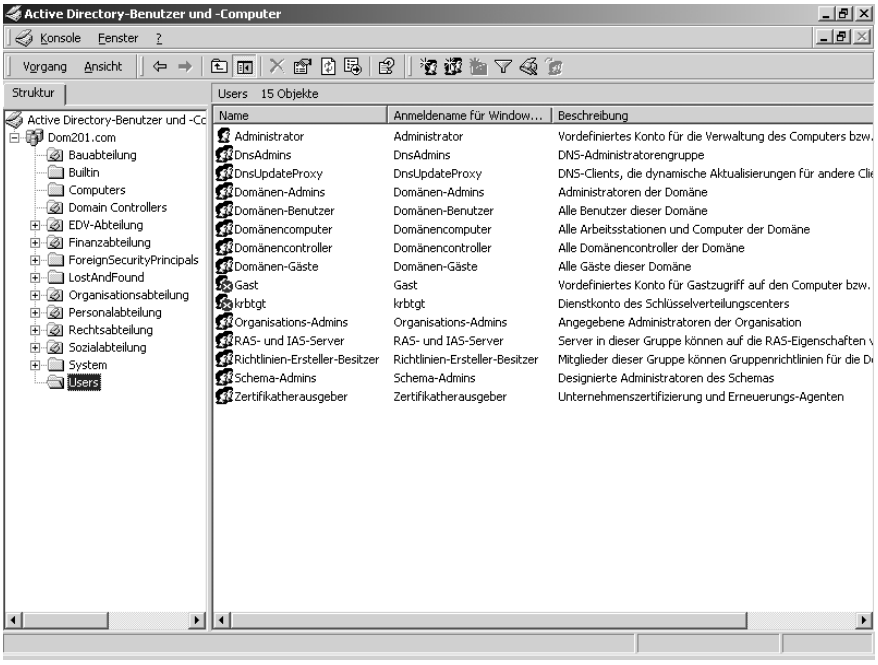
Active Directory-Benutzer und -Computer – Container *Builtin*

Der Hauptzweck der Gruppen im Container *Builtin* besteht darin, die Kompatibilität mit Windows NT sicherzustellen. Es sollten deshalb in diesem Container keine neuen Benutzer- und Gruppenkonten angelegt werden.

Gruppe	**Beschreibung**
Administratoren	Diese Gruppe hat Vollzugriff auf die Domäne, nicht aber auf andere Domänen im Domänenbaum. Mitglieder sind die Benutzer- und Gruppenkonten *Administrator*, *Domänen-Admins* und *Organisations-Admins*.
Benutzer	Die Mitglieder dieser Gruppe haben Benutzerrechte im System. Sie können mit dem System arbeiten und Dokumente speichern. Die Installation von Software oder die Konfiguration des Systems ist nicht möglich. Mitglieder dieser Gruppe sind *Authentifizierte Benutzer*, *Domänen-Benutzer* und *Interaktiv*.

Druckoperatoren	Die Mitglieder dieser Gruppe können Drucker verwalten.
Gäste	Mitglieder dieser Gruppe können mit dem Computer eingeschränkt arbeiten und Dokumente speichern. Die Gruppe sollte aus Sicherheitsgründen nicht verwendet werden. Das zugehörige Benutzerkonto *Gast* ist standardmäßig deaktiviert.
Kontenoperatoren	Die Mitglieder können Benutzer-, Gruppen- und Computerkonten verwalten.
Prä-Windows 2000-kompatibler Zugriff	Eine mit Vorgängerversionen kompatible Gruppe, die allen Benutzern und Gruppen in der Domäne Zugriff ermöglicht. Mitglied ist allein die Gruppe *Jeder*.
Replikationsoperatoren	Die Gruppe unterstützt die Dateireplikation in Domänen.
Serveroperatoren	Die Mitglieder können Domänenserver verwalten.
Sicherungsoperatoren	Sicherungsoperatoren können Sicherheitseinschränkungen lediglich zum Sichern oder Wiederherstellen von Dateien außer Kraft setzen.

6.4.2 Die Benutzer- und Gruppenkonten im Container *Users*



Active Directory-Benutzer und -Computer – Container *Users*

Der Container *Users* enthält überwiegend Benutzer-, Gruppen- und Computerkonten, die von Windows 2000 standardmäßig für administrative Zwecke eingerichtet wurden. Die Verwaltung dieser Konten ist nicht an den Container gebunden, sodass die Benutzer- und Gruppenkonten auch in andere Container bzw. Organisationseinheiten verschoben werden können.

Benutzer	**Beschreibung**
Administrator	Dieses Benutzerkonto ist in einer Root-Domäne das wichtigste und kritischste Konto. Es erlaubt den administrativen Zugriff auf alle Funktionen und Daten und ist Mitglied der Gruppen *Administratoren*, *Domänen-Admins*, *Domänen-Benutzer*, *Organisations-Admins*, *Richtlinien-Ersteller-Besitzer* und *Schema-Admins*. Im Regelfall sollte dieses Konto im täglichen Betrieb nicht verwendet werden. Stattdessen sollten zusätzliche Administratorenkonten für die verschiedenen anfallenden Aufgaben eingerichtet werden.
Gast	Das Benutzerkonto *Gast* erlaubt den eingeschränkten Zugriff auf das System. Standardmäßig ist es gesperrt. Aus Sicherheitsgründen sollte es nicht verwendet werden.
Krbtgt	Das Konto *Krbtgt* ist das Dienstkonto des Kerberos Key Distribution Center (Schlüsselverteilungscenter). Es ist standardmäßig gesperrt.

Gruppe	**Beschreibung**
DnsAdmins	Die Gruppe *DnsAdmins* enthält die Administratoren für DNS-Server. Dieser Gruppe sind standardmäßig keine Benutzer zugeordnet. Sie kann verwendet werden, um die Administration von DNS-Servern zu delegieren.
DnsUpdateProxy	In der Gruppe *DnsUpdateProxy* befinden sich Computer, die als Proxy für die dynamische Aktualisierung von DNS-Einträgen fungieren können.
Domänen-Admins	Die Gruppe *Domänen-Admins* enthält die Administratoren-Benutzerkonten.

Gruppe	Beschreibung
Domänen-Benutzer	In der Gruppe *Domänen-Benutzer* befinden sich alle Benutzerkonten der Domäne. Wird ein neues Benutzerkonto angelegt, wird es automatisch Mitglied dieser Gruppe. Deshalb sollten dieser Gruppe nur dann Zugriffsrechte zugeordnet werden, wenn die Berechtigungen in gleicher Weise für alle Benutzer gelten.
Domänencomputer	In dieser Gruppe befinden sich alle Computer der Domäne.
Domänencontroller	Die Gruppe *Domänencontroller* ist eine spezielle Gruppe, in die alle Domänencontroller aufgenommen werden. Sie wird für die Zuweisung von Zugriffsberechtigungen für die Kommunikation zwischen Domänencontrollern benötigt.
Domänen-Gäste	Die Gruppe *Domänen-Gäste* enthält alle Gastkonten einer Domäne. Sie sollte aus Sicherheitsgründen nicht verwendet werden.
Organisations-Admins	Die Gruppe *Organisations-Admins* ist eine spezielle Gruppe, die das Active Directory verwaltet. Mitglied dieser Gruppe ist das Administratorkonto.
RAS- und IAS-Server	In dieser Gruppe befinden sich alle Computerkonten, auf denen der RAS (Remote Access Service) oder der IAS (Internetauthentifizierungsdienst) ausgeführt wird.
Richtlinien-Ersteller-Besitzer	Die Gruppe *Richtlinien-Ersteller-Besitzer* umfasst die Benutzerkonten, die Gruppenrichtlinien für die Domäne erstellen dürfen.
Schema-Admins	Mitglieder der Gruppe *Schema-Admins* können Veränderungen am Schema des Active Directory vornehmen. Mitglied dieser Gruppe ist wiederum das Administratorkonto.
Zertifikatherausgeber	Mit der Gruppe *Zertifikatherausgeber* ist die Verwaltung von digitalen Zertifikaten verbunden.

Bei untergeordneten Domänen in einem Domänenbaum gibt es einige Unterschiede in Bezug auf die standardmäßig definierten Gruppen. Nur die Root-Domäne enthält Gruppen, die administrativ die gesamte Domänenstruktur (Forest) verwalten können.

Folgende Gruppen werden ausschließlich in der Root-Domäne definiert:

- DnsUpdateProxy,
- Organisations-Admins,
- Schema-Admins,
- DnsAdmins.

Um den administrativen Aufwand zu reduzieren, ist es wichtig, die Domänen in der richtigen Reihenfolge einzurichten. Die für die Domänengesamtstruktur zuständigen Administratoren sollten zum ersten eingerichteten Domänenbaum (Root-Domäne) gehören.

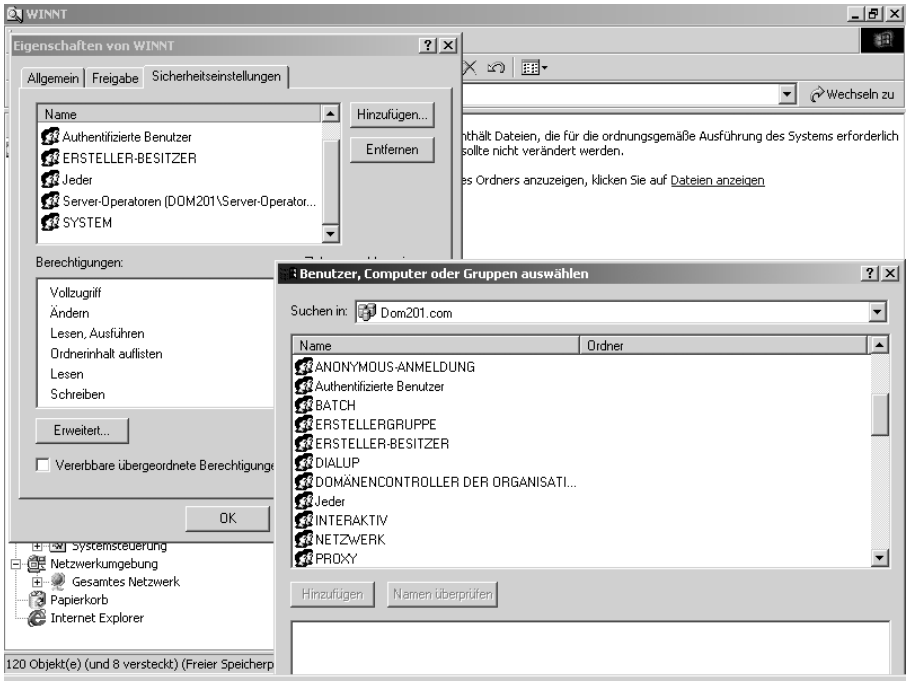
Analysieren Sie genau die Gruppenmitgliedschaften, damit Sie bei der Verwaltung der Ressourcen bzw. der Objekte (Ordner, Dateien) darüber informiert sind, welches Benutzerkonto über welche Befugnisse verfügt.

6.4.3 Spezielle Systemgruppen

Vordefinierte Systemgruppen, die auch als **Sondergruppen** bezeichnet werden, verfügen über keine bestimmten Mitgliedschaften und werden deshalb nicht im Active Directory verwaltet. Sie werden von Windows 2000 automatisch den Ressourcen zugewiesen, können aber bei der Zuweisung von Rechten, z. B. auf einen Ordner, über die Registerkarte *Sicherheitseinstellungen* administriert werden. In der nachfolgenden Tabelle werden die am häufigsten verwendeten vordefinierten Systemgruppen beschrieben:

Gruppe	**Beschreibung**
Jeder	Die Gruppe *Jeder* umfasst alle Benutzer, die auf den Computer zugreifen. Diese Gruppe sollte nur dann einer Ressource zugeordnet werden, wenn alle Benutzer auf diese zugreifen dürfen.
Authentifizierte Benutzer	Alle Benutzer, die über ein gültiges Benutzerkonto verfügen, sind Mitglieder dieser Gruppe. Insofern ist sie mit der Gruppe *Jeder* zu vergleichen.
ERSTELLER-BESITZER	Die Gruppe beinhaltet das Benutzerkonto des Benutzers, der eine Ressource erstellt oder deren Besitz übernommen hat.

Netzwerk	In der Gruppe *Netzwerk* befinden sich alle Benutzerkonten, die von einem anderen Computer im Netzwerk mit einer freigegebenen Ressource des „eigenen“ Computers verbunden sind.
Interaktiv	Die Gruppe *Interaktiv* beinhaltet das Benutzerkonto des Benutzers, der an dem Computer angemeldet ist. Er erhält Zugriff auf alle Ressourcen des Computers.
ANONYMUS-ANMELDUNG	Die Gruppe ANONYMUS-ANMELDUNG enthält Benutzerkonten, die Windows 2000 nicht authentifiziert. Benutzername und Kennwort sind nicht erforderlich. Diese Art von Anmeldung wird beim Einsatz des Internet Information Server unterstützt.
SYSTEM	Dies ist eine Gruppe, die Windows 2000 für die Ausführung des Betriebssystems benötigt. Sie wird allen Betriebssystemressourcen (Ordner Winnt) zugeordnet.
DIALUP	Diese Gruppe enthält Benutzerkonten, die über Wählverbindungen zugreifen.



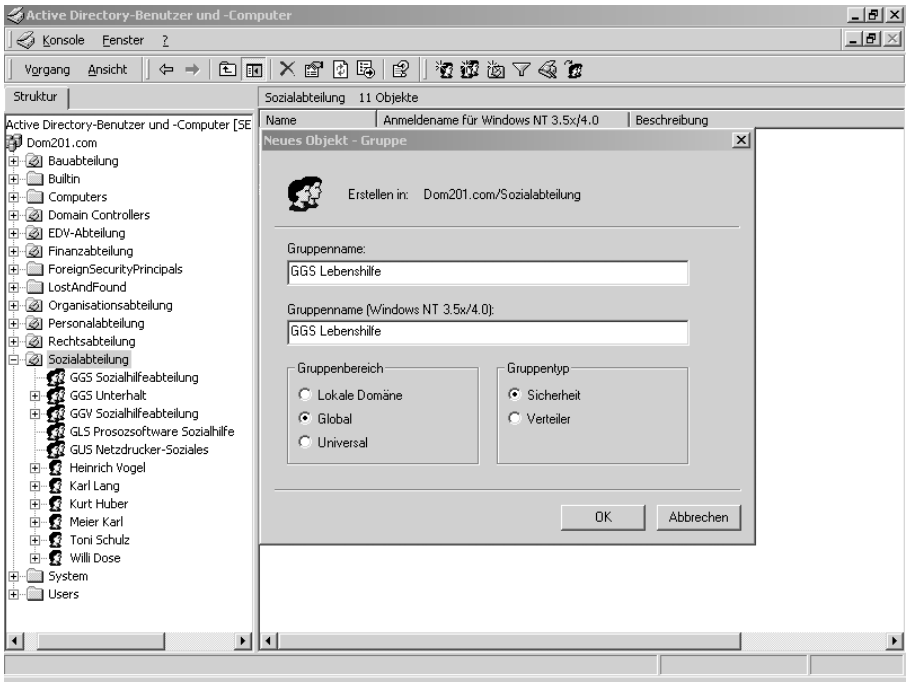
Systemgruppen

6.4.4 Gruppenkonten verwalten

Mit der Erstellung von Gruppenkonten wird die Zuweisung von Zugriffsrechten erheblich vereinfacht, weil die einem Gruppenkonto zugewiesenen Mitglieder (Benutzer- oder/und Gruppenkonten) automatisch die Berechtigungen der Gruppe erhalten. Die Mitgliedschaften der Benutzer- und Gruppenkonten können sehr differenziert vergeben werden.

Darüber hinaus muss beim Anlegen einer Gruppe bestimmt werden, welchem Gruppenbereich und Gruppentyp sie zugeordnet werden soll. Windows 2000 unterstützt

- lokale Domänen-Gruppen,
- globale Gruppen und
- universelle Gruppen.



Anlegen einer globalen Gruppe

Lokale Domäne	**Beschreibung**
Mitgliedschaft	Es können Mitglieder aus einer beliebigen Domäne der Domänengesamtstruktur hinzugefügt werden.

Zugriff auf Ressourcen	Der lokalen Gruppe können nur Berechtigungen auf Ressourcen zugewiesen werden, die sich in der gleichen Domäne befinden, in der die Gruppe angelegt wurde.
Betriebsmodus	Keine Einschränkungen.

Global	**Beschreibung**
Mitgliedschaft	Es können nur Mitglieder aus der Domäne hinzugefügt werden, in der die globale Gruppe erstellt wurde.
Zugriff auf Ressourcen	Der Gruppe können Berechtigungen auf Ressourcen zugewiesen werden, die sich in beliebigen Domänen befinden.
Betriebsmodus	Keine Einschränkungen.

Universell	**Beschreibung**
Mitgliedschaft	Es können Mitglieder aus einer beliebigen Domäne der Domänengesamtstruktur hinzugefügt werden.
Zugriff auf Ressourcen	Es können der Gruppe Berechtigungen auf Ressourcen zugewiesen werden, die sich in einer beliebigen Domäne befinden.
Betriebsmodus	Universelle Gruppen sind im gemischten Modus nicht verfügbar. Alle Windows 2000-Funktionen werden nur im einheitlichen Modus unterstützt.

Gruppentyp *Sicherheit* und *Verteiler*

Der Gruppentyp *Sicherheit* unterstützt im Gegensatz zu dem Gruppentyp *Verteiler* die Zuweisung von Berechtigungen auf eine Ressource. Sollen beispielsweise die Mitglieder einer neu angelegten Gruppe auf einen Ordner lesenden Zugriff erhalten, muss sie als Gruppentyp *Sicherheit* definiert werden. Eine angelegte Gruppe mit dem Gruppentyp *Verteiler* wird nicht für die Berechtigungszuweisung unter Sicherheitseinstellungen aufgeführt. Verteilergruppen haben nur dann eine Bedeutung, wenn keine Sicherheitseinstellungen benötigt werden, wie z. B. bei einem E-Mail-Verteiler.

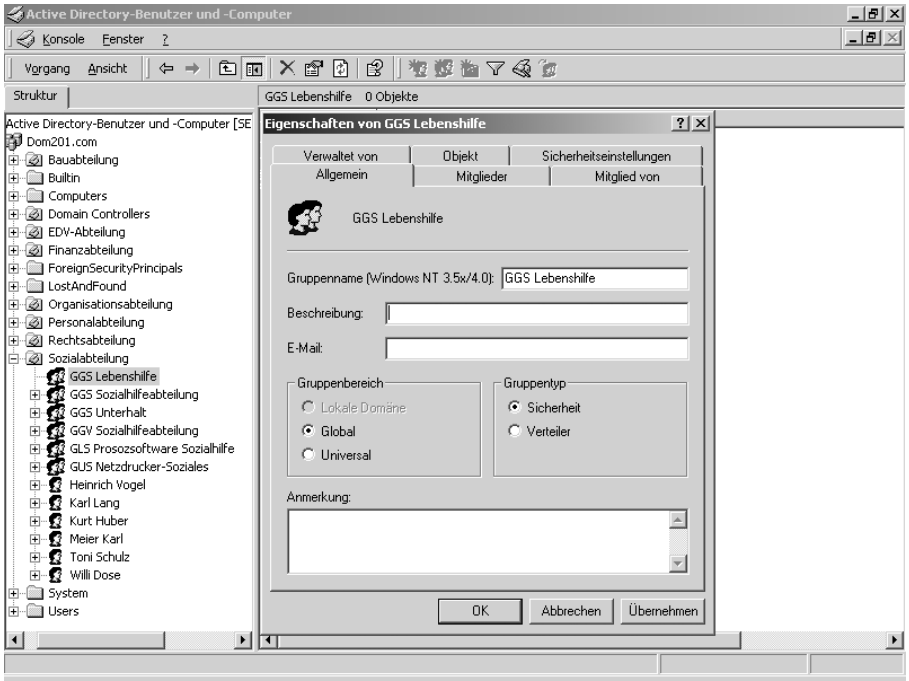
Anlegen eines Gruppenkontos!

1. *Klicken Sie mit der rechten Maustaste auf eine Organisationseinheit, in der Sie eine Gruppe anlegen möchten.*
2. *Zeigen Sie auf NEU und klicken Sie dann auf GRUPPE.*
3. *Es öffnet sich ein Dialogfenster, in dem Sie den GRUPPENNAMEN, den GRUPPENBEREICH und den GRUPPENTYP erfassen können.*

Wie bei den Benutzerkonten können die Eigenschaften eines Gruppenkontos erst nach dem Anlegen administriert werden.

Eigenschaften eines Gruppenkontos administrieren!

1. *Klicken Sie mit der rechten Maustaste auf ein Gruppenkonto.*
2. *Wählen Sie EIGENSCHAFTEN und bestätigen Sie mit der linken Maustaste.*
3. *Es öffnet sich ein Eigenschaftenfenster mit der aktiven Registerkarte ALLGEMEIN.*



Eigenschaften eines Gruppenkontos – Registerkarte Allgemein

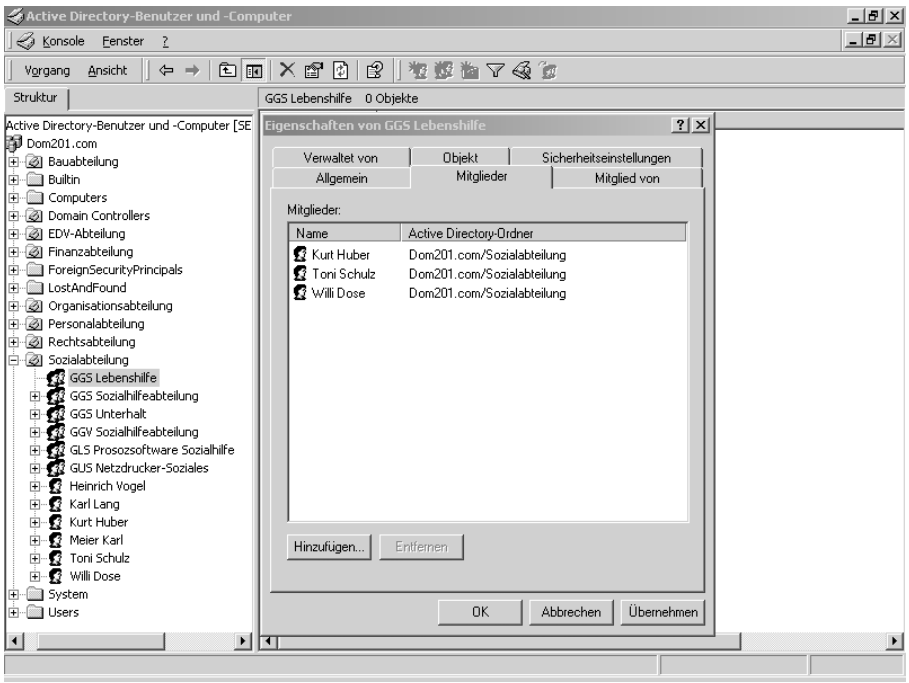
Registerkarte *Allgemein*

Auf der Registerkarte *Allgemein* können der Gruppenbereich oder der Gruppentyp geändert werden. Weiterhin lassen sich nähere Erläuterungen oder Hinweise zu der Gruppe in einem gesonderten Feld unterbringen. Sofern der gewählte Gruppenname auf NT-Clients nicht unterstützt wird, kann ein abweichender Gruppenname vergeben werden.

- Die Änderung des Gruppenbereichs ist nur in Domänen im einheitlichen Modus möglich.
- Eine globale Gruppe kann nur in eine universelle Gruppe geändert werden, wenn die globale Gruppe kein Mitglied einer anderen globalen Gruppe ist.
- Eine lokale Domänengruppe kann nur in eine universelle Gruppe geändert werden, wenn sie keine andere lokale Domänengruppe enthält.

Registerkarten *Mitglieder* und *Mitglied von*

Unter diesen Registerkarten werden die Mitgliedschaften verwaltet. Über die Registerkarte *Mitglieder* können der Gruppe Benutzer- und/oder Gruppenkonten zugewiesen werden, während unter der Registerkarte *Mitglied von* die Gruppe selbst Mitglied anderer Gruppen werden kann.



Eigenschaften eines Gruppenkontos – Registerkarte Mitglieder

Wenn Sie mehrere Benutzerkonten oder Gruppen hinzufügen möchten, können Sie diese einzeln auswählen und mit HINZUFÜGEN bestätigen. Sie können aber auch die Umschalt- oder Steuerungstaste gedrückt halten, um mehrere Benutzerkonten oder Gruppen zu markieren. Mit der Umschalttaste können Sie aufeinander folgende Konten auswählen, während Sie bei der Verwendung der Steuerungstaste einzelne Konten auswählen und andere überspringen können.

Registerkarte *Verwaltet von*

Auf der Registerkarte *Verwaltet von* können Informationen über den Benutzer/Administrator abgelegt werden, der die Aufgabe hat, Gruppenkonten zu verwalten. Es kann hier nur das entsprechende Benutzerkonto eingetragen werden. Informationen, die unter dem Benutzerkonto z. B. auf der Registerkarte *Allgemein* eingetragen wurden, werden dann in die Datenfelder der Registerkarte *Verwaltet von* übertragen.

Registerkarten Objekt und Sicherheitseinstellungen

Die Registerkarten *Objekt* und *Sicherheitseinstellungen* verfügen über die gleichen Funktionen wie die der Benutzerkonten (siehe Tz. 6.3). Auf der Registerkarte *Objekt* werden Informationen über die Objektklasse, das Erstellungs- und Änderungsdatum sowie die Original-USN (Unique Sequence Number) sowie die aktuelle USN verwaltet, während mithilfe der Registerkarte *Sicherheitseinstellungen* Berechtigungen für die Administration des Gruppenkontos vergeben werden können.

6.4.5 Gruppenstrategien und Gruppenmitgliedschaftsregeln

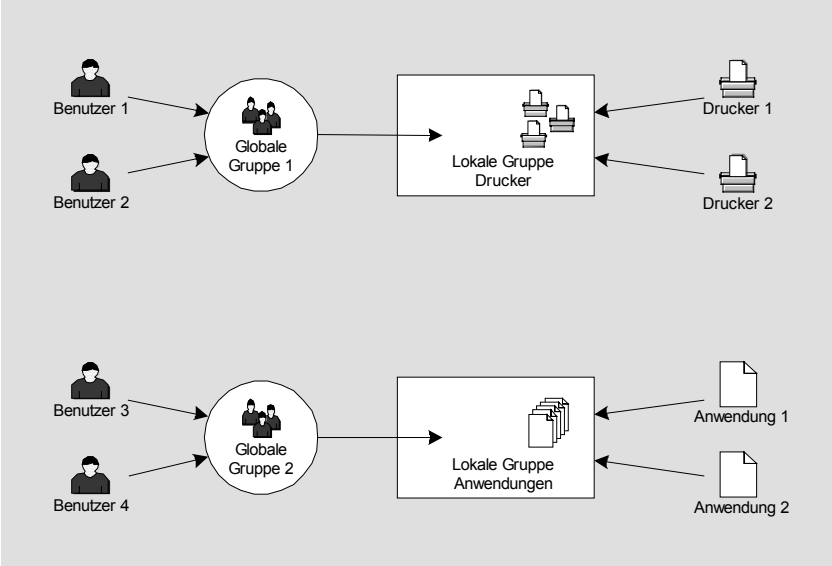
Der Gruppenbereich bestimmt die Mitgliedschaft der Gruppe. **Mitgliedschaftsregeln** definieren, welche Mitglieder eine Gruppe enthalten kann. In der nachstehenden Tabelle werden die Gruppenmitgliedschaftsregeln in Abhängigkeit vom Betriebsmodus aufgeführt:

Gruppenbereich	**Mitgliedskonten im gemischten Modus**	**Mitgliedskonten im einheitlichen Modus**
Lokale Domäne	Benutzerkonten Computerkonten Globale Gruppen	Benutzerkonten Computerkonten Lokale Domänengruppen Globale Gruppen Universelle Gruppen

Global	Benutzerkonten Computerkonten	Benutzerkonten Computerkonten Globale Gruppen
Universell	Nicht verfügbar im gemischten Modus	Benutzerkonten Computerkonten Globale Gruppen Universelle Gruppen

Die **Gruppenmitgliedschaften** haben erheblichen Einfluss darauf, welche Aktion ein Benutzer im Netzwerk und auf einem PC ausführen kann. Durch das Hinzufügen eines Benutzerkontos zu einer Gruppe wird der Benutzer zum Mitglied und erhält somit sämtliche Berechtigungen der Gruppe.

Eine sinnvolle **Strategie** Gruppen anzulegen wäre z. B., eine globale Gruppe der Benutzer einer Abteilung mit gleichen Aufgaben zu bilden. Globale Gruppen spiegeln dementsprechend den **Geschäftsverteilungsplan** der Organisation wieder. Lokale Gruppen sollten zur Vereinfachung der Zuweisung von Zugriffsrechten auf die Datenbestände und sonstigen Ressourcen angelegt werden, d. h., die im Netzwerk befindlichen Ressourcen (Drucker, Fachanwendungen, Datenablagen) verfügen jeweils über eine lokale Gruppe, die mit dem Namen der jeweiligen Ressource bezeichnet wird.



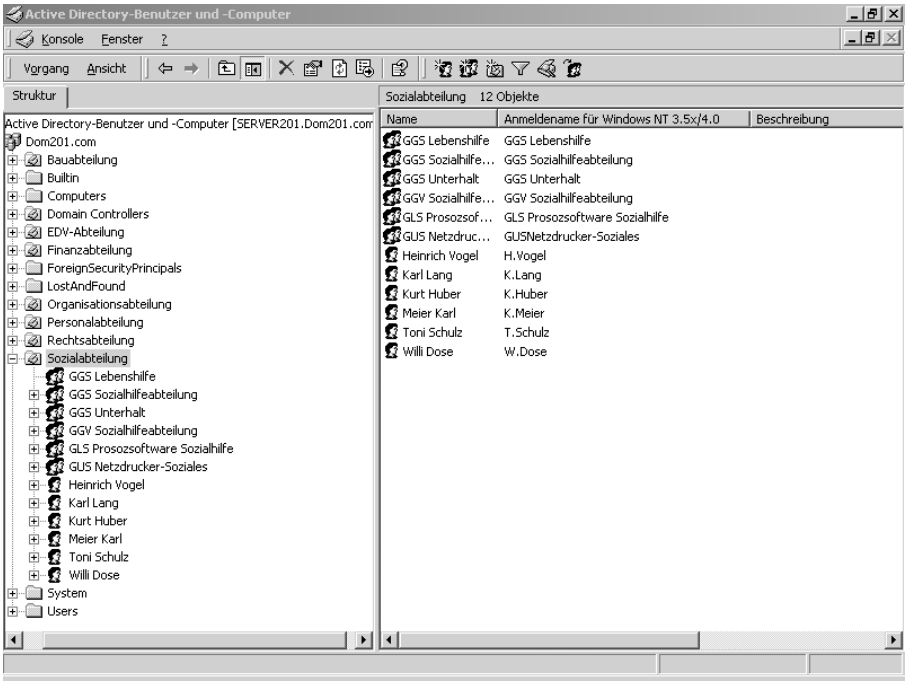
Gruppenstrategie

Ein Benutzer erhält Zugriff auf eine Ressource, indem z. B. die globale Gruppe „Abteilung1“, in der er Mitglied ist, der lokalen Gruppe „Fachanwendung1“ zugeordnet wird. Das hat u. a.

den Vorteil, dass bereits über die **Gruppenverwaltung** erkennbar ist, welche Benutzer welche Ressourcen nutzen.

Der Einsatz universeller Gruppen macht nur dann Sinn, wenn Benutzern der Zugriff auf Ressourcen in mehreren Domänen gewährt werden muss. Ist also erkennbar, dass eine Ressource domänenübergreifend zum Einsatz kommt, kann ihr eine universelle Gruppe zugeordnet werden. Ist z. B. ein Benutzer der Domäne A Mitglied der universellen Gruppe „Abteilung1“, und ist diese Gruppe einer Ressource in Domäne B zugeordnet, dann kann der Benutzer auf diese Ressource zugreifen.

Universelle Gruppen können in einer Domänenstruktur zu einem hohen Netzwerkverkehr zwischen Domänencontrollern führen, wenn Sie die Mitgliedschaft der Gruppe ändern, da jede Änderung das Replizieren der Active Directory-Datenbank auf andere Domänencontroller verursacht.



Gruppenkennzeichnung für Gruppenbereich und Gruppentyp

Beachten Sie, dass die Gruppenbereiche (lokale, globale und universelle Gruppen) grafisch nicht **differenziert** im Active Directory angezeigt werden. Sie können deshalb anhand des Gruppensymbols nicht erkennen, um welchen Gruppenbereich und Gruppentyp es sich handelt. Aus diesem Grund wird für eine bessere Strukturierung empfohlen, eine Kennzeichnung mit in der Gruppennamensvergabe aufzunehmen, z. B.

GGS für **G**ruppe **G**lobal **S**icherheit,

GLS für **G**ruppe **L**okal **S**icherheit,

GUS für **G**ruppe **U**niversal **S**icherheit oder

GGV für **G**ruppe **G**lobal **V**erteiler (siehe Abbildung).

Eine nach diesen Kriterien durchgeführte Kennzeichnung hat auch den Vorteil, dass über die Active Directory-Suchfunktionen ein gezielteres Auffinden der Gruppe möglich ist.

- Um eine effektive Nutzung von Gruppen zu gewährleisten, müssen Sie bestimmen, wie Sie diese einsetzen werden und welche Art von Gruppe in bestimmten Situationen verwendet wird.
- Sie sollten die Gruppenmitgliedschaften dokumentieren, um Berechtigungszuweisungen verfolgen zu können.
- Versuchen Sie die Verschachtelungsebenen auf ein Minimum zu reduzieren, wenn Sie Gruppen anderen Gruppen hinzufügen.

6.5 Sicherheitscheck

- *Planen Sie die Benutzer- und Gruppenverwaltung **sorgfältig**.*
- *Legen Sie fest, nach welchen **Kriterien** Sie Benutzer- und Gruppenkonten anlegen wollen.*
- *Berücksichtigen Sie, dass Windows 2000 über keine **Reportfunktionen** für die Gruppenmitgliedschaften und die den Benutzer- und Gruppenkonten zugewiesenen Berechtigungen verfügt.*
- ***Dokumentieren** Sie deshalb die Benutzer- und Gruppenverwaltung z. B. über das Tool DUMPSEC (siehe Kapitel 11).*
- *Prüfen Sie **regelmäßig**, ob die angelegten Benutzer- und Gruppenkonten sowie die zugewiesenen Mitgliedschaften den Vorgaben entsprechen.*
- *Machen Sie sich mit den von Windows 2000 standardmäßig eingerichteten Benutzer- und Gruppenkonten vertraut. Überprüfen Sie die **Mitgliedschaften**.*

- *Benennen Sie das Administratorkonto so um, dass über die Benutzerkennung **nicht** auf ein Administratorkonto geschlossen werden kann.*
- *Beachten Sie, dass das **Administratorkonto** der Root-Domäne in den Gruppenkonten DOMÄNEN-ADMINS, SCHEMA-ADMINS und ORGANISATONS-ADMINS Mitglied ist.*
- *Legen Sie für jeden Administrator ein **eigenständiges** Benutzerkonto an.*
- *Aktivieren Sie beim **Anlegen** neuer Benutzerkonten das Kontrollkästchen BENUTZER MUSS KENNWORT BEI DER NÄCHSTEN ANMELDUNG ÄNDERN.*
- *Legen Sie für die Benutzerkonten **einheitlich** fest, welche Einstellungen, z. B. Profil oder Anmeldezeiten, auf den einzelnen Registerkarten vorgenommen werden sollen.*
- *Beachten Sie, dass die speziellen **Systemgruppen** JEDER und AUTHENTIFIZIERTE BENUTZER alle Benutzerkonten umfassen.*
- *Legen Sie die Gruppenkonten so an, dass **globale** Gruppen Ihre Organisation und **lokale** Gruppen die Ressourcen repräsentieren. Verwenden Sie universelle Gruppen nur, wenn Sie domänenübergreifend auf Ressourcen zugreifen.*
- ***Kennzeichnen** Sie in der Namensvergabe die Gruppen nach Gruppenbereich und Gruppentyp.*
- *Geben Sie für die Benutzer- und Gruppenkonten im Feld BESCHREIBUNG an, zu welcher **Abteilung** sie gehören.*
- *Legen Sie fest, welcher Administrator die **Berechtigungen** für die Benutzer- und Gruppenkontenverwaltung erhält.*

7 Benutzerprofile und Basisordner

In diesem Kapitel erfahren Sie,

- welche Bedeutung und Strukturen Benutzerprofile haben,
- den Unterschied zwischen lokalen, serverbasierten und verbindlichen Benutzerprofilen,
- wie Benutzerprofile erstellt, kopiert und gelöscht werden,
- welche Vorteile serverbasierte Benutzerprofile haben,
- mit welchen Gruppenrichtlinien die Benutzerprofile eingeschränkt werden können und
- warum Basisordner für die Verwaltung von Daten wichtig sind.

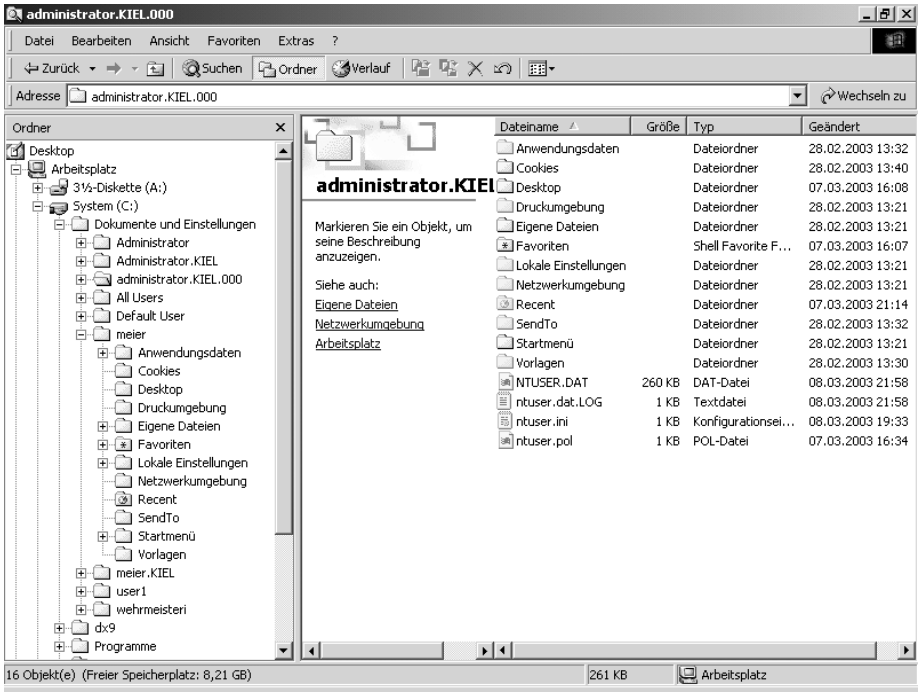
7.1 Bedeutung und Struktur des Benutzerprofils

Ein Benutzerprofil wird in einem **eigenständigen Ordner** für jedes **Benutzerkonto** beim erstmaligen Anmelden an einem Computer automatisch erstellt. Der Ordner erhält immer den **Anmeldenamen** des entsprechenden Benutzerkontos. Unter Windows NT werden die Benutzerprofile unter dem Ordner <\winnt\Profiles> erstellt und verwaltet. Windows 2000 hat den Speicherort für die Benutzerprofile außerhalb des Betriebssystemordners in das Verzeichnis **<Stammverzeichnis:\Dokumente und Einstellungen>** gelegt. Melden sich Benutzer an ihren Arbeitsstationen an, werden die ursprünglich individuell festgelegten Desktop-Einstellungen wiederhergestellt. Mehrere Benutzer können deshalb denselben Computer verwenden und haben dennoch ihre „eigene“ Benutzerumgebung.

In Bezug auf die Funktion der Benutzerprofile unterscheidet man

- lokale Benutzerprofile,
- servergespeicherte Benutzerprofile und
- verbindliche servergespeicherte Benutzerprofile.

Lokale Benutzerprofile werden lokal auf dem Computer gespeichert, an dem sich der Benutzer anmeldet, während ein servergespeichertes Benutzerprofil auf einem Server gespeichert wird. Ein verbindliches servergespeichertes Benutzerprofil kann vom Benutzer nicht verändert werden. Es wird deshalb vorwiegend für eine Benutzergruppe eingerichtet.



Benutzerprofilstrukturen

Wenn sich ein Benutzer zum ersten Mal am Client anmeldet, prüft Windows 2000 zunächst, ob der Benutzer ein lokales oder ein serverbasiertes Profil besitzt. Danach wird geprüft, ob ein **Standard-Netzwerk-Benutzerprofil** DEFAULT USER im Ordner <Stammverzeichnis:\Winnt\Sysvol\Sysvol\<Domänenname>\Scripts> des Domänencontrollers vorhanden ist. Wenn kein Standard-Netzwerk-Benutzerprofil existiert, wird das lokale Standard-Benutzerprofil DEFAULT USERS in ein Profil mit dem Namen des Benutzers kopiert und im Ordner <Stammverzeichnis:\Dokumente und Einstellungen> gespeichert. Danach wird im Standard-Benutzerprofil ALL USERS nach Einstellungen gesucht, die zusätzlich für den Benutzer übernommen werden sollen (Änderungen am ALL USERS-Profil werden sofort in die Benutzerprofile der Benutzer übernommen und wirken bei der nächsten Anmeldung).

Lokale und servergespeicherte Benutzerprofile besitzen die gleiche Struktur. Ein servergespeichertes Benutzerprofil wird bei der Anmeldung am Client heruntergeladen (kopiert) und in dem Ordner <Stammverzeichnis:\Dokumente und Einstellungen> gespeichert. Beim Abmelden wird das Benutzerprofil dann auf den Server zurückgespeichert.

- Bei servergespeicherten Benutzerprofilen kann der Ordner EIGENE DATEIEN eine hohe Netzwerklast erzeugen. Die gesamten Profilstrukturen werden bei jeder Benutzeranmeldung auf den Client kopiert. Meldet sich der Benutzer vom Client ab, wird das Benutzerprofil wiederum über das Netzwerk auf dem Server abgelegt.

- Über die Gruppenrichtlinien können für das Benutzerprofil, wie z. B. die Deaktivierung der Zwischenspeicherung, Einschränkungen vorgenommen werden.

Die Ordner und Dateien des Benutzerprofils haben folgende Bedeutung:

Benutzerprofilordner	**Inhalt**
Anwendungsdaten	spezifische Konfigurationsdateien der Anwendungen
Cookies	Cookies der Internetnutzung
Desktop	Desktop-Elemente sowie Dateien und Verknüpfungen
Druckerumgebung	Verknüpfungen zu Elementen im Druckerordner
Eigene Dateien	Benutzerdateien, z. B. Worddateien (Standardablage)
Eigene Bilder	vom Benutzer erstellte Bilddateien
Favoriten	Verknüpfungen für Programmelemente und bevorzugte Speicherorte
Lokale Einstellungen	benutzerspezifische Konfigurationsdateien für Anwendungen (z. B. temporäre Internetdateien)
Netzwerkumgebung	Verknüpfungen für Elemente der Netzwerkumgebung
Recent	Verknüpfungen zu Dateien, auf die zuletzt zugegriffen wurde
SendTo	Verknüpfungen für Dokumentelemente
Startmenü	Programmverknüpfungen der Menüeinträge, die unter START-PROGRAMME angezeigt werden
Vorlagen	Vorlagen für ältere Office-Anwendungen

Benutzerprofildatei	**Inhalt**
Ntuser.dat	Diese Datei enthält die Registrierungsstruktur für einen Benutzer.

	Sie wird in die Registrierung geladen, wenn sich der Benutzer anmeldet, und wird zu einem Unterbaum des Schlüssels Hkey_Current_User.
Ntuser.dat.log	Diese Transaktionsdatei enthält die aktuellen Änderungen eines Benutzerprofils und dient der Fehlertoleranz.
Ntuser.ini	Hier werden Initialisierungseinstellungen für Terminaldienste abgelegt.
Ntuser.pol	Diese Datei dient als lokaler Zwischenspeicher für benutzerbasierte Gruppenrichtlinien, die von einem Domänencontroller heruntergeladen werden, wenn sich ein Benutzer an der Domäne anmeldet.

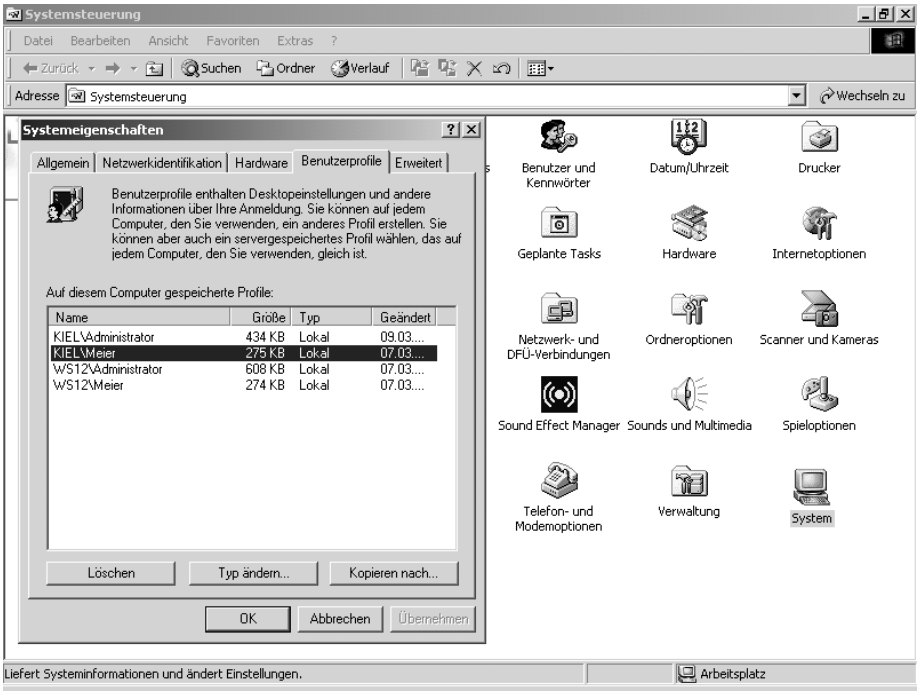
Um alle Ordner und Dateien des Benutzerprofils anzuzeigen, muss über den Explorer die Ordneransicht ALLE DATEIEN UND ORDNER ANZEIGEN aktiviert werden (EXTRA-ORDNEROPTIONEN-ANSICHT).

Unter Windows 2000 trägt der oberste Ordner eines Profils denselben Namen wie der Anmeldename des Benutzerkontos. Dieser entsteht, wenn sich der Benutzer lokal am Computer anmeldet. Meldet sich der Benutzer hingegen an der Domäne an, wird der Name des Ordners zusätzlich mit dem Domänennamen und ggf. mit der Endung „000“ versehen (siehe Abbildung). Als NTFS-Berechtigungen werden für das lokale Benutzerprofil dem entsprechenden Benutzerkonto und der lokalen Gruppe *Administratoren* Vollzugriffsrechte zugewiesen. Auf dem Serverprofil erhält hingegen nur das Benutzerkonto Vollzugriffsrechte. Die Administratoren verfügen bei serverbasierten Benutzerprofilen nur über die Möglichkeit der Besitzübernahme (siehe Kapitel 8).

7.2 Benutzerprofile verwalten

Es gibt Fälle, in denen es erforderlich ist, ein lokales Benutzerprofil auf einen anderen Benutzer zu übertragen. Wenn die Einstellungen einer Desktop-Oberfläche (eingerichtete Anwendungen, Einschränkungen der Systemfunktionen) für mehrere Benutzer gelten sollen, sollte zunächst ein Musterbenutzerprofil entwickelt werden. Dieses kann dann einzelnen Benutzerkonten zugewiesen werden, ohne dass das Benutzerprofil erneut konfiguriert werden muss.

Da die Benutzerprofile Bestandteil der Registrierung sind, darf ein Benutzerprofil nicht über den Explorer kopiert werden. Es wird deshalb unter der Systemsteuerung eine Funktion unterstützt, über die Benutzerprofile verwaltet werden können.



Benutzerprofil verwalten

Unter der Registerkarte BENUTZERPROFILE werden alle auf dem entsprechenden Computer verfügbaren Benutzerprofile angezeigt. Diese befinden sich im Ordner DOKUMENTE UND EINSTELLUNGEN. Über die Registerkarte können die Benutzerprofile gelöscht, kopiert oder der Typ in ein servergespeichertes Profil geändert werden.

Löschen eines lokalen Benutzerprofils!

1. *Zeigen Sie auf START-EINSTELLUNGEN-SYSTEMSTEUERUNG und doppelklicken Sie auf SYSTEM oder klicken Sie mit der rechten Maustaste auf ARBEITSPLATZ und wählen Sie aus dem Kontextmenü EIGENSCHAFTEN.*

2. *In dem Fenster SYSTEMEIGENSCHAFTEN klicken Sie auf die Registerkarte BENUTZERPROFILE.*

3. *Klicken Sie auf das zu löschende Benutzerprofil und wählen Sie danach die Option LÖSCHEN.*

4. *Bestätigen Sie die Sicherheitsabfrage mit JA, das Benutzerprofil wird vom System automatisch aus dem Ordner DOKUMENTE UND EINSTELLUNGEN und aus der Registrierung gelöscht.*

Kopieren eines lokalen Benutzerprofils!

1. *Klicken Sie auf das zu kopierende Benutzerprofil und wählen Sie danach die Option KOPIEREN.*

2. *In dem neu geöffneten Fenster geben Sie in dem Feld PROFIL KOPIEREN NACH zunächst den Ordner (Speicherort) an, in den das Benutzerprofil kopiert werden soll.*

3. *Klicken Sie danach auf die Schaltfläche (Benutzer) ÄNDERN. Es öffnet sich ein weiteres Fenster mit den in der Domäne eingerichteten Benutzer- und Gruppenkonten.*

4. *Wählen Sie ein Benutzer- oder Gruppenkonto aus. Bestätigen Sie anschließend mit OK, und das ausgewählte Benutzerprofil wird kopiert.*

7.3 Serverbasierte Benutzerprofile einrichten

Bevor serverbasierte Benutzerprofile eingerichtet werden, sollten folgende Fragen geklärt werden:

Melden sich die Benutzer sowohl auf Windows 2000/NT- als auch bei Windows 9x-Computern an?

Da Windows 9x über eine andere Profilstruktur verfügt, sollten die Windows 9x-Profile in einem gesonderten Ordner verwaltet werden.

Speichern die Benutzer zahlreiche Dateien unter ihren lokalen Profilen, z. B. im Ordner EIGENE DATEIEN, ab?

Die Profilgröße sollte zunächst überprüft werden. Für die Speicherung von Dateien sollte ein Basisordner eingerichtet werden (siehe Tz. 7.5).

Melden sich die Benutzer bei mehreren Computern gleichzeitig an?

Ist das der Fall, können Dateien verloren gehen bzw. überschrieben werden.

Gibt es Netzwerk- und Speicherengpässe auf dem „Profilserver“?

Wenn sich morgens zahlreiche Benutzer am Computer anmelden, wird der Profilserver durch das Herunterladen der Profile besonders beansprucht. Der Server sollte über ausreichende Kapazitäten verfügen.

Arbeiten die Benutzer mit verschlüsselten Ordnern bzw. Dateien?

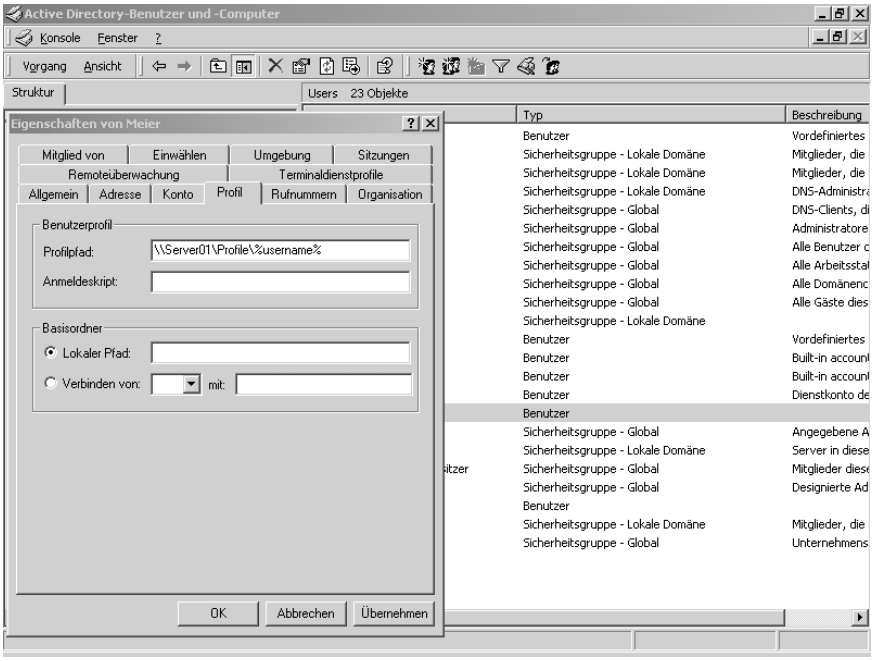
Verschlüsselte Dateien (siehe Tz. 8.6) lassen sich im servergespeicherten Benutzerprofil eines Benutzers speichern. Allerdings kann das Profil bei der Anmeldung nicht mehr auf den Client kopiert werden. Es erscheint eine Fehlermeldung. Verschlüsselte Dateien sollten deshalb in einem **Basisordner** verwaltet werden.

Servergespeicherte Profile einrichten!

1. *Auf dem Server ist zunächst ein Profilordner, z. B. mit dem Namen PROFILE, anzulegen. Für den Ordner ist eine versteckte Freigabe einzurichten.*
2. *Öffnen Sie die Konsole des ACTIVE DIRECTORY-BENUTZER UND -COMPUTER.*
3. *Klicken Sie mit der rechten Maustaste auf das gewünschte Benutzerobjekt und wählen Sie im Kontextmenü die Option EIGENSCHAFTEN.*
4. *Aktivieren Sie die Registerkarte PROFIL.*
5. *Geben Sie im Feld PROFILPFAD den Pfad zum freigegebenen Ordner auf dem Profilserver ein. Der Pfad wird wie folgt angegeben:*

   \\Servername\Freigabename des Ordners\%username%

6. *Klicken Sie auf OK, um die Änderungen zu speichern. Der Pfad auf dem Profilserver wird eingerichtet, wenn sich der Benutzer das nächste Mal anmeldet. Das Profil wird jedoch erst beim Abmelden auf den Profilserver kopiert.*



Registerkarte Profil des Benutzerkontos Meier

Ein verbindliches serverbasiertes Benutzerprofil wird einfach durch die Umbenennung der Datei NTUSER.DAT in NTUSER.MAN (mandatory = zwingend) erstellt. Danach ist das serverbasierte Benutzerprofil geschützt. Die Benutzer können zwar während der Anmeldung Änderungen am Desktop vornehmen, diese werden jedoch nicht auf dem Profilserver gespeichert. Bei erneuter Anmeldung erhält der Benutzer wieder das auf dem Server verbindliche Benutzerprofil.

7.4 Gruppenrichtlinien für Benutzerprofile

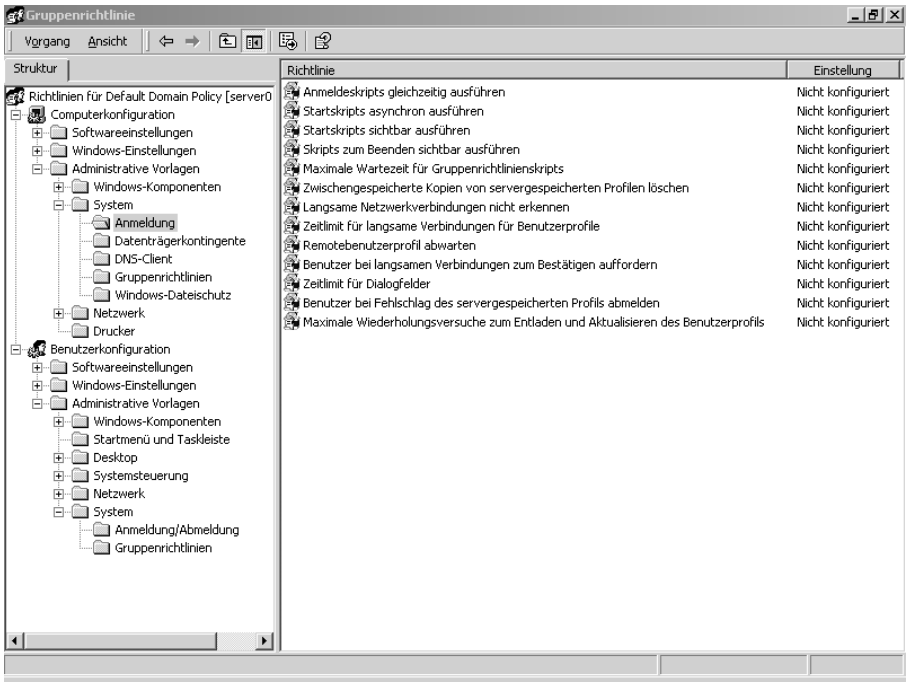
Unter den Gruppenrichtlinien (siehe Kapitel 10) befinden sich u. a. folgende Einstellungsmöglichkeiten für die Verwaltung der Benutzerprofile:

- Zwischengespeicherte Kopien von servergespeicherten Profilen löschen

  Die vom Profilserver auf den Client heruntergeladenen Profile werden nach der Abmeldung des Benutzers auf dem Client gelöscht.

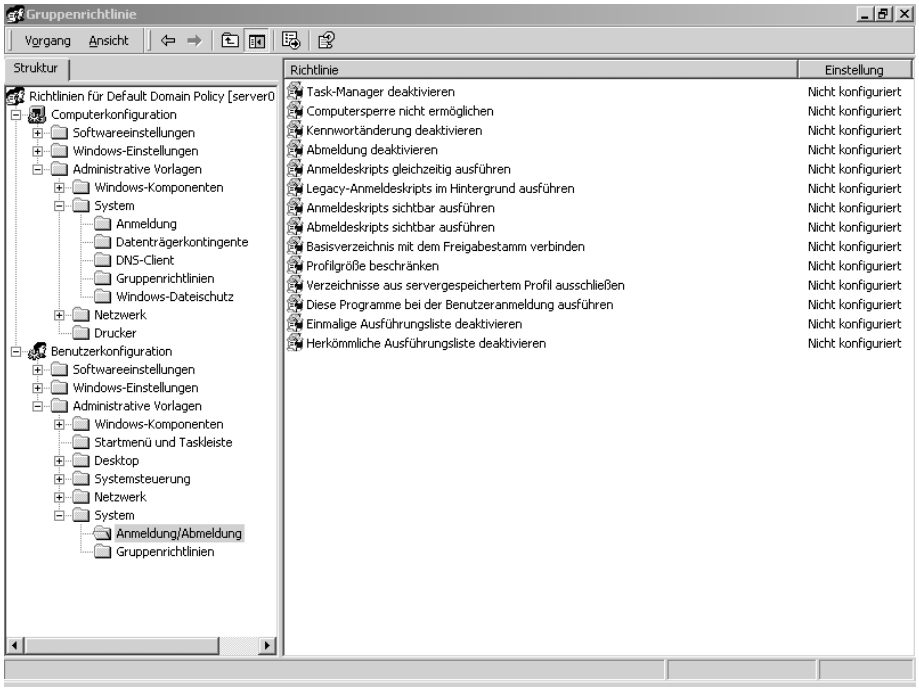
- Benutzer bei Fehlschlag des servergespeicherten Profils abmelden

  Kann das servergespeicherte Benutzerprofil des Benutzers nicht geladen werden, wird der Benutzer automatisch abgemeldet.



Gruppenrichtlinien für Benutzerprofile – Computerkonfiguration

Diese Richtlinie ist hilfreich, wenn ein servergespeichertes Benutzerprofil nicht gefunden werden kann oder das Profil fehlerhaft ist und daher nicht ordnungsgemäß geladen werden kann. Wenn diese Richtlinie deaktiviert oder nicht konfiguriert ist, wird, falls das servergespeicherte Profil fehlschlägt, eine lokale Kopie (falls vorhanden) des servergespeicherten Benutzerprofils geladen. Ansonsten wird das Standard-Benutzerprofil, das unter <Stammverzeichnis:\Dokumente und Einstellungen\Default User> gespeichert wird, geladen.



Gruppenrichtlinien für Benutzerprofile – Benutzerkonfiguration

- Profilgröße beschränken

  Erreicht ein servergespeichertes Benutzerprofil die maximale Größe, kann festgelegt werden, welche Vorgänge ausgeführt werden sollen (z. B. Benachrichtigung des Benutzers). Wenn diese Richtlinie nicht aktiv ist, wird die zugelassene Größe der servergespeicherten Benutzerprofile nicht eingeschränkt.

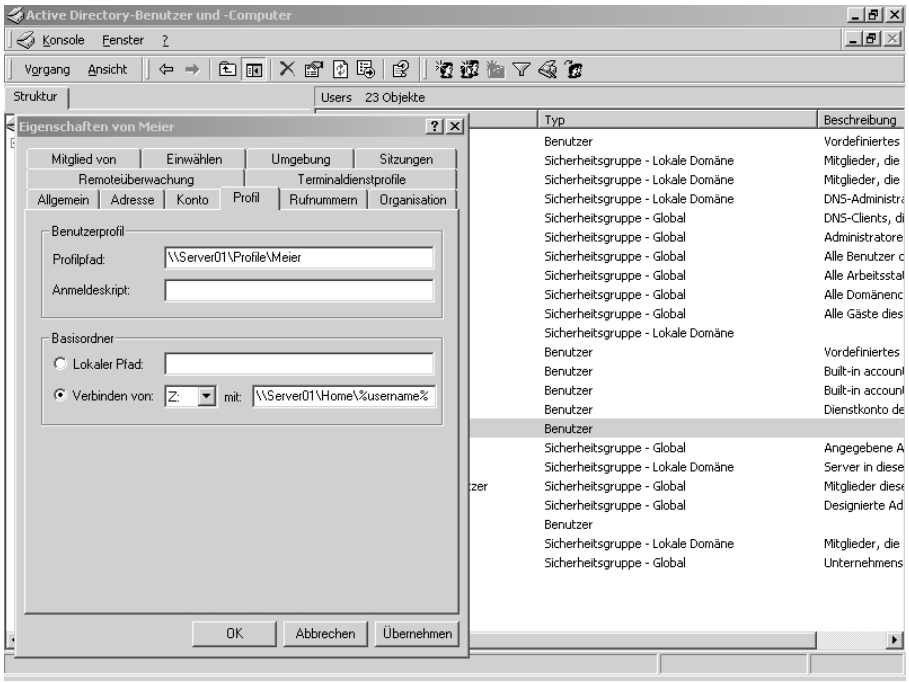
- Verzeichnisse aus serverbasiertem Profil ausschließen

  Mithilfe dieser Richtlinie können Ordner ausgeschlossen werden, die normalerweise Teil des Benutzerprofils sind. Standardmäßig werden die Ordner VERLAUF, LOKALE EINSTELLUNGEN, TEMP und TEMPORÄRE INTERNET DATEIEN aus dem servergespeicherten Benutzerprofil ausgeschlossen. Durch das Aktivieren dieser Richtlinie können zusätzliche Ordner ausgeschlossen werden.

7.5 Arbeits- bzw. Basisordner

In einem Basisordner lassen sich Daten in vorgegebenen Ordnerstrukturen auf einem Server speichern. Basisordner werden in zwei Schritten eingerichtet:

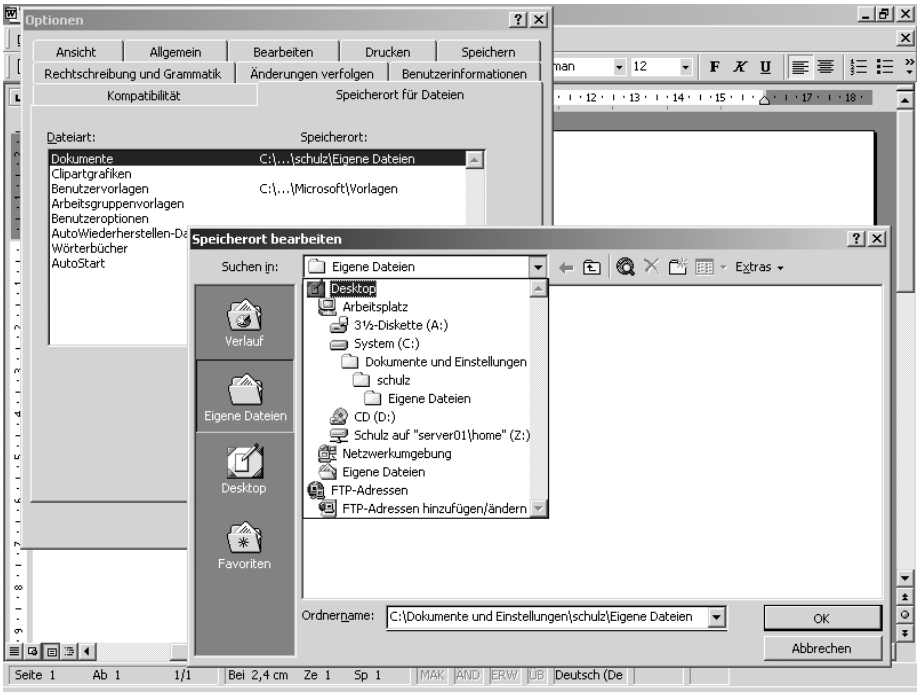
- Auf dem Server muss ein freigegebener Ordner für die Basisordner eingerichtet werden.
- Das Benutzerkonto muss so eingerichtet werden, dass es auf den Basisordner verweist.



Benutzerkonto Meier – Basisordner

Nachdem auf der Registerkarte PROFIL des Benutzerkontos der entsprechende Pfad für den Basisordner eingetragen wurde, wird automatisch ein Ordner mit dem Anmeldenamen des Benutzerkontos erzeugt. Auf den Ordner erhalten das entsprechende Benutzerkonto und die Gruppe *Administratoren* Vollzugriff. Es wird empfohlen, eine Struktur zu schaffen, unter der **alle Basisordner** der Benutzer verwaltet werden. Wird eine der Organisation angepasste Ablagestruktur (siehe Kapitel 8) erstellt, kann der Basisordner auch in diese integriert werden.

Damit der Benutzer **automatisch** bei der Nutzung von Standardsoftware auch „seinen“ Basisordner verwenden kann, sollte der Speicherort in der jeweiligen Standardsoftware vorgegeben werden. Bearbeitet der Benutzer dann z. B. ein Worddokument, wird es automatisch beim Speichern in „seinen“ Basisordner abgelegt.



Word, Konfiguration des Speicherorts

Basisordner verwalten!

1. *Erstellen Sie auf dem Server einen Ordner (z. B. Home) für die Basisordner und geben Sie ihn frei.*

2. *Öffnen Sie das Snap-In ACTIVE DIRECTORY-BENUTZER UND -COMPUTER.*

3. *Klicken Sie mit der rechten Maustaste auf das gewünschte Benutzerobjekt und wählen Sie im Kontextmenü die Option EIGENSCHAFTEN.*

4. *Aktivieren Sie die Registerkarte PROFIL.*

5. *Geben Sie im Feld VERBINDEN VON den Pfad zum freigegebenen Basisordner auf dem Server ein. Der Pfad wird wie folgt angegeben: Z: mit <\\Servername\Freigabename des Ordners für Basisordner\%username%>*

6. *Klicken Sie auf OK, um die Änderungen zu speichern. Der Basisordner wird auf dem Server sofort eingerichtet.*

Mit der Verwaltung von Basisordnern sollten Sie auch den Einsatz der Datenträgerkontingente berücksichtigen. Damit gewährleisten Sie, dass die Benutzer nur beschränkten Speicherplatz innerhalb „ihres“ Ordners erhalten, sodass eine übermäßige Speicherung von Dateien in Grenzen gehalten wird (siehe Kapitel 8).

7.6 Sicherheitscheck

- *Beziehen Sie bei der Verwaltung der Benutzerkonten auch die **Benutzerprofile** mit ein.*
- *Damit ein Benutzer immer seine individuelle Desktop-Oberfläche erhält, sollten Sie **serverbasierte** Benutzerprofile einrichten.*
- *Legen Sie für die Benutzerprofile einen gesonderten Ordner mit einer **versteckten** Freigabe an.*
- *Beachten Sie, dass ausreichender **Speicherplatz** auf dem Server für die Benutzerprofile zur Verfügung steht.*
- *Nehmen Sie ggf. Einstellungen in den Gruppenrichtlinien vor, damit die Benutzerprofile **einheitlich** verwaltet werden (siehe Kapitel 10).*
- *Berücksichtigen Sie, dass ein Benutzer bei der Verwendung servergespeicherter Benutzerprofile Fehlermeldungen bei der **Verschlüsselung** von Dateien innerhalb seines Profilordners erhält.*
- *Erstellen Sie für den Benutzer deshalb einen **Basisordner** außerhalb der Profilstrukturen, in dem der Benutzer auch verschlüsselte Dateien unproblematisch ablegen kann.*
- *Setzen Sie mit der Verwaltung der Basisordner die Funktion der **Datenträgerkontingente** ein (siehe Kapitel 8).*

8 Zugriffsberechtigungen

In diesem Kapitel erfahren Sie,

- wie Sie den Zugriff auf Ressourcen und Daten über Berechtigungen steuern,
- was der Unterschied zwischen Freigabe- und NTFS-Berechtigungen ist,
- welchen Ressourcen Freigabeberechtigungen zugewiesen werden können,
- wie viele verdeckte „Standardfreigaben“ bereits existieren,
- welche Bedeutung NTFS-Berechtigungen haben und wie sie administriert werden,
- wie eine zentrale Datenablage mit NTFS-Berechtigungen abgeschottet wird,
- wann die Verschlüsselung (EFS) von Ordnern und Dateien sinnvoll sein kann und
- wie für Benutzer Datenträgerkontingente eingerichtet werden können.

8.1 Zugriffskontrolle auf Ressourcen

Unter Windows 2000 erfolgt die Zugriffskontrolle auf Ressourcen auf **zwei Ebenen**. Zunächst benötigt der Benutzer **Benutzer- bzw. Systemrechte** (siehe Tz. 9.4.2), die es ihm erlauben, die Systemfunktionen des Computers zu nutzen. Erhält der Benutzer das Recht, sich an einem Computer anzumelden, können ihm darüber hinaus **Zugriffsrechte** (Freigabe- und NTFS-Berechtigungen) auf ausgewählte Ressourcen (Ordner, Dateien, Drucker) des lokalen Computers oder der im Netzwerk befindlichen Computer erteilt bzw. verwehrt werden.

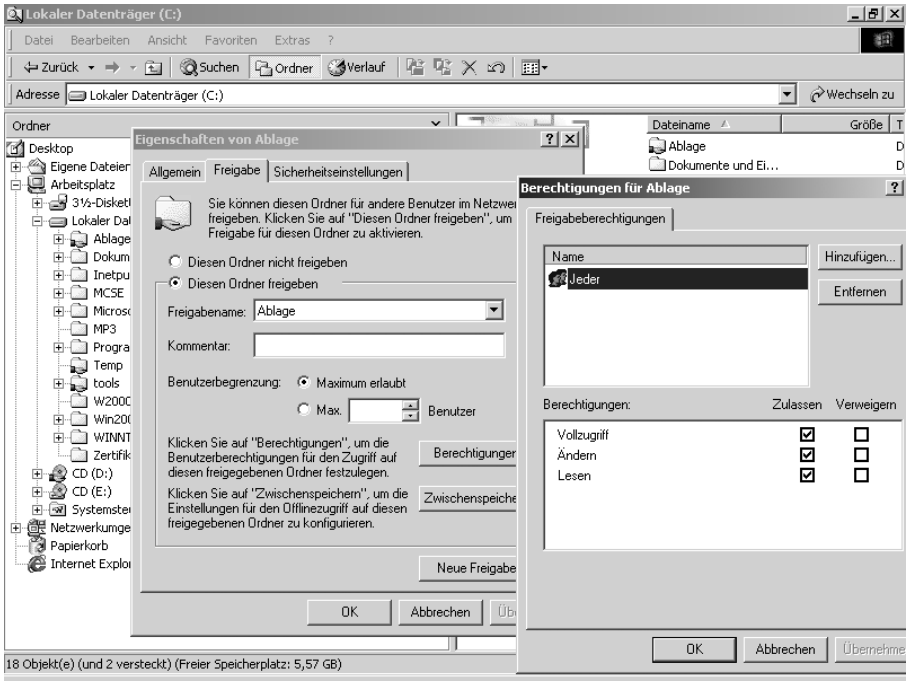
Die auf verschiedenen Ebenen den Benutzer- und Gruppenkonten erteilten Zugriffsberechtigungen können in ihrer Gesamtheit nicht transparent gemacht werden. Windows 2000 verfügt über keine **Reportfunktionen**, die z. B. alle einem Benutzerkonto zugewiesenen Berechtigungen sichtbar macht, um die ordnungsgemäße Zuweisung von Berechtigungen zu überprüfen. Es wird deshalb empfohlen, ein Tool einzusetzen, dass die Revision der Administration der Zugriffsberechtigungen unterstützt (siehe Kapitel 11).

In der Reihenfolge der Berücksichtigung der Berechtigungen stehen die Benutzerrechte (Systemrechte) vor den Zugriffsrechten (Freigabe- und NTFS-Berechtigungen).

8.2 Freigabeberechtigungen

Freigabeberechtigungen werden verwendet, damit Benutzer im **Netzwerk** auf Ressourcen zugreifen können. Wird z. B. ein Ordner freigegeben, können die Benutzer über das Netzwerk eine Verbindung zu diesem Ordner herstellen und erhalten so Zugriff auf die enthaltenen Dateien. Freigabeberechtigungen können vergeben werden für

- Drucker,
- Laufwerke (CD-ROM, Diskettenlaufwerk, Festplatte) und
- Ordner.



Freigabe mit dem Explorer erstellen

Eine freigegebene Ressource wird im *Windows Explorer* als **Symbol** mit einer Hand, die den freigegebenen Ordner hält, dargestellt.

Folgendes ist bei der Verwaltung von Freigabeberechtigungen zu beachten:

- *Um die Zugriffsverwaltung einfacher zu gestalten, sollten Sie Freigabeberechtigungen nur Gruppenkonten zuweisen.*
- *Ermitteln Sie, welche Gruppen Zugriff auf welche Ressourcen haben müssen und welche Zugriffsbefugnisse erforderlich sind.*
- *Dokumentieren Sie die Gruppen und ihre Berechtigungen für jede Ressource.*
- *Verwenden Sie nachvollziehbare Freigabenamen, sodass Administratoren die Ressourcen einfach erkennen und suchen können.*
- *Der Benutzer sollte über keine Funktionen verfügen, mit denen ein Zugriff auf die Netzwerkumgebung ermöglicht wird. Daher sollten Sie aus Sicherheitsgründen die Netzwerkverbindungen auf die freigegebenen Ressourcen in die Desktop-Oberfläche der entsprechenden Benutzer integrieren.*

Mit der Erteilung einer Freigabe können über den *Explorer* folgende Optionen gewählt werden:

Option	**Beschreibung**
Diesen Ordner nicht freigeben	Der Ordner wird nicht freigegeben, und alle weiteren Optionen werden ausgeblendet bzw. deaktiviert.
Diesen Ordner freigeben	Der Ordner wird freigegeben, und alle weiteren Optionen sind administrierbar.
Freigabename	Der Name der Freigabe wird angezeigt, der den Benutzern für die Verbindung mit der Ressource angezeigt wird. Der vorgeschlagene Name kann geändert werden.
Kommentar	Ein Kommentar kann optional eingegeben werden. Er wird zusätzlich zum Freigabenamen angezeigt. Er kann verwendet werden, um z. B. den Inhalt eines freigegebenen Ordners zu kennzeichnen.
Benutzerbegrenzung	Die Anzahl der Benutzer kann bestimmt werden, die gleichzeitig eine Verbindung zur freigegebenen Ressource herstellen können.
Berechtigungen	Es können Berechtigungen für freigegebene Ressourcen vergeben werden. Sie gelten nur, wenn über das Netzwerk auf die Res-

	source zugegriffen wird. Standardmäßig wird der Gruppe *Jeder* *Vollzugriff* gewährt.
Zwischenspeichern	Offline zur Verfügung gestellte Dateien können in einem Zwischenspeicher (Cache) abgelegt werden, wenn der Computer für die Verwendung von Offlinedateien eingerichtet ist. Der Zwischenspeicher kann an dieser Stelle konfiguriert werden.
Neue Freigabe erstellen	Ist ein Ordner mindestens 1 x freigegeben, wird diese Option verfügbar. Es kann dann eine weitere Freigabe auf diesen Ordner erstellt werden.
Freigabe entfernen	Ist ein Ordner mehrfach freigegeben, wird diese Option verfügbar. Es können dann einzelne Freigaben gelöscht werden.

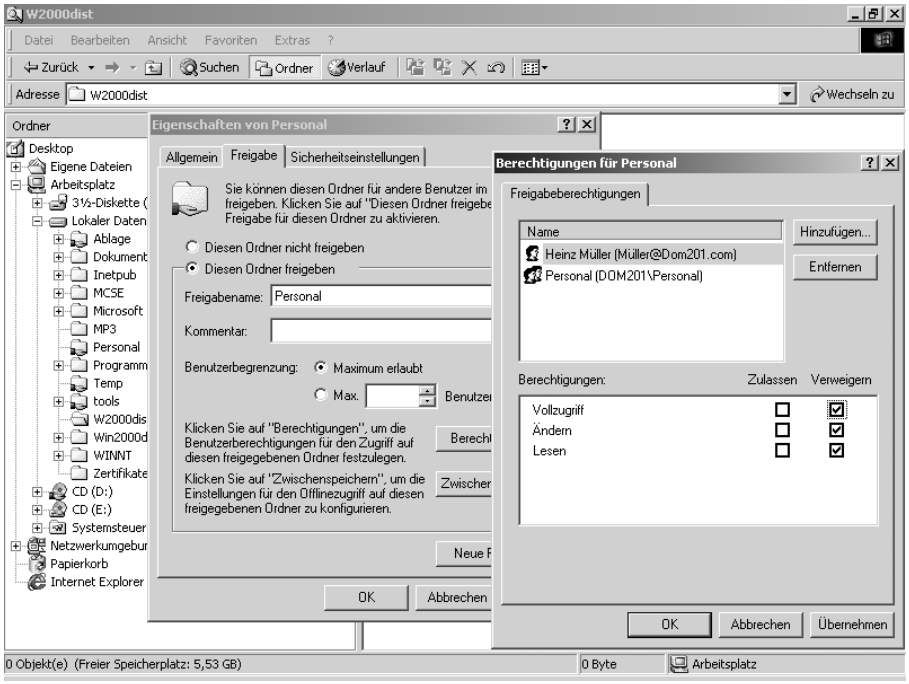
Bei Auswahl der Schaltfläche BERECHTIGUNGEN auf der Registerkarte FREIGABE können folgende Freigabeberechtigungen vergeben werden:

Berechtigung	**Beschreibung**
Vollzugriff	Benutzer können die Dateiberechtigungen ändern, den Besitz von Dateien übernehmen sowie alle Aktionen durchführen, die unter der Berechtigung *Ändern* möglich sind.
Ändern	Benutzer können Ordner erstellen, Dateien zu Ordnern hinzufügen, Daten in Dateien ändern, Dateiattribute ändern, Ordner und Dateien löschen sowie Programme ausführen.
Lesen	Benutzer können Ordner- und Dateinamen sowie Attribute anzeigen. Programme können ausgeführt werden.

Berechtigungen für freigegebene Ordner beziehen sich auf Ordner und **nicht** auf einzelne Dateien. Da Berechtigungen nicht auf einzelne Dateien bezogen werden können, bieten sie keine **ausreichende** Sicherheit.

Verweigerte Berechtigungen setzen Berechtigungen außer Kraft, die einem Benutzerkonto oder einer Gruppe auf einem anderen Wege gewährt wurden. Wenn z. B. der Ordner „Personal“ für ein Gruppenkonto freigegeben wurde, erhalten automatisch alle Mitglieder (Benut-

zerkonten) den Zugriff auf die entsprechenden Ressourcen. Soll jedoch einem einzelnen Mitglied dieser Gruppe der Zugriff verweigert werden, ist das entsprechende Benutzerkonto



dem Ordner „Personal“ mit Verweigerungsrechten zuzuordnen.

Freigabeberechtigungen für ein Benutzerkonto verweigern

Windows 2000 gibt Ordner zu Verwaltungszwecken automatisch frei. An diese Freigabe wird das Dollarzeichen ($) angefügt. Das Dollarzeichen blendet die freigegebene Ressource im Explorer aus. In der folgenden Tabelle wird der Zweck der administrativen freigegebenen Ordner beschrieben, die von Windows 2000 automatisch generiert werden.

Freigabe	**Zweck**
C$, D$, E$ usw.	Das Stammverzeichnis jedes Laufwerks auf der Festplatte wird automatisch freigegeben. Der Freigabename ist der Laufwerkbuchstabe gefolgt von einem Dollarzeichen ($). Wenn der Administrator eine Verbindung zu diesem Ordner aufbaut, kann er auf den gesamten Datenträger zugreifen.
Admin$	Der Systemstammordner (standardmäßig C:\Winnt) wird als Admin$ freigegeben. Administratoren können auf diesen freigegebenen Ordner mit der Berechtigung *Vollzugriff* zugreifen, ohne dass ihnen der Name des Ordners bekannt sein muss.

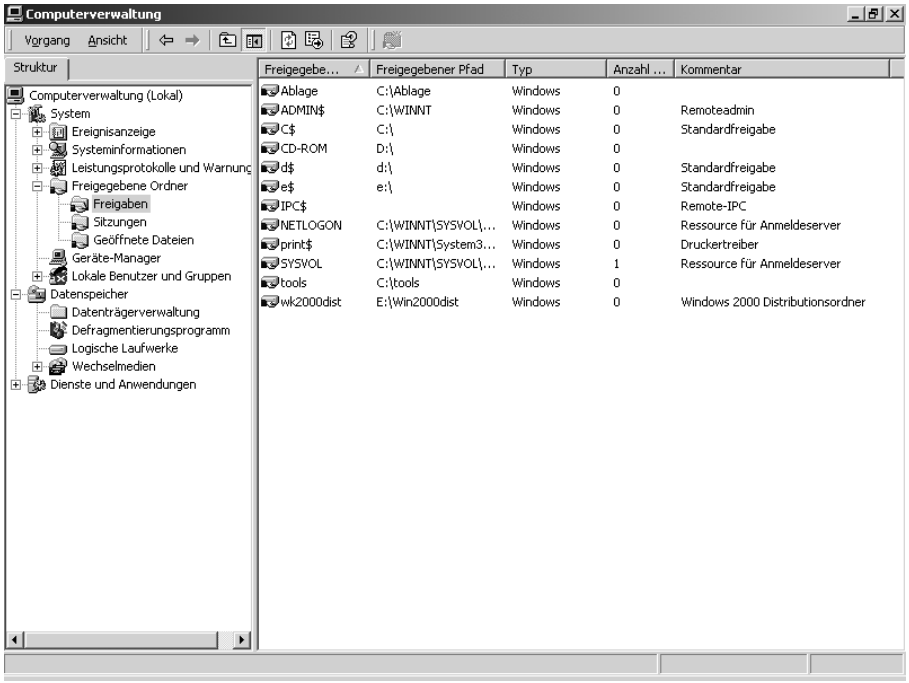
Print$	Bei der Installation des ersten freigegebenen Druckers wird der Ordner <%systemroot%\System32\Spool\Drivers> als *Print$* freigegeben. Dieser Ordner stellt den Zugriff auf die Dateien mit Druckertreibern für Clients bereit. Nur Mitglieder der Gruppen *Administratoren*, *Server-Operatoren* und *Druck-Operatoren* verfügen über die Berechtigung *Vollzugriff*. Die Gruppe *Jeder* verfügt über eine *Leseberechtigung*.

Einen Ordner für den Zugriff über das Netz mithilfe des Explorers freigeben!

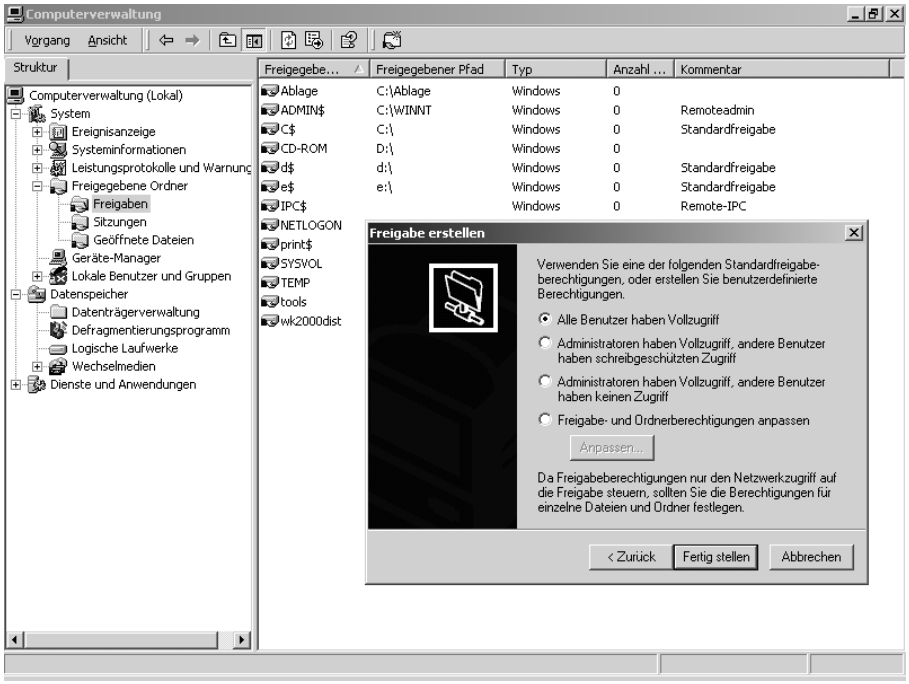
1. *Rufen Sie den Explorer auf.*
2. *Klicken Sie zum Freigeben eines Ordners mit der rechten Maustaste auf den gewünschten Ordner und wählen Sie* FREIGABE.
3. *Klicken Sie auf* DIESEN ORDNER FREIGEBEN *und ändern Sie ggf. den vorgegebenen Freigabenamen.*
4. *Sofern Sie eine ausgeblendete (versteckte) Freigabe erstellen wollen, fügen Sie hinter dem Freigabenamen ein Dollarzeichen an.*
5. *Da dem Ordner standardmäßig die Gruppe* JEDER *mit der Berechtigung* VOLLZUGRIFF *zugewiesen wird, ändern Sie ggf. mit der Option* BERECHTIGUNGEN *die Berechtigungen auf das erforderliche Maß.*
6. *Bestätigen Sie mit OK und überprüfen Sie Ihre Berechtigungszuweisungen, indem Sie sich unter einem Benutzerkonto anmelden und auf die freigegebene Ressource zugreifen.*

- Greift ein Benutzer auf einen freigegebenen Ordner zu, der sich auf dem gleichen Computer befindet, an dem er angemeldet ist, dann wird der Zugriff nicht beschränkt. Berechtigungen für freigegebene Ordner gelten nur für Benutzer, die über das **Netzwerk** eine Verbindung zu dem Ordner herstellen.
- Wenn Sie einen Ordner freigeben, wird ihm standardmäßig die Gruppe *Jeder* mit der Berechtigung *Vollzugriff* zugewiesen.

Mit dem Verwaltungsprogramm *Computerverwaltung* können die auf dem Computer eingerichteten und ausgeblendeten Freigaben administriert werden.



Computerverwaltung, Freigegebene Ordner



Computerverwaltung, Freigabe erstellen

Einen Ordner mithilfe der Computerverwaltung freigeben!

1. *Rufen Sie über START-PROGRAMME-VERWALTUNG die COMPUTERVERWALTUNG auf.*
2. *Doppelklicken Sie auf FREIGEGEBENE ORDNER und danach mit der rechten Maustaste auf FREIGABEN.*

3. *Wählen Sie NEUE DATEIFREIGABE oder NEU-DATEIFREIGABE.*

4. *Geben Sie den Ordnernamen ein oder wählen Sie DURCHSUCHEN, um die Ressource zu bestimmen, die Sie freigeben möchten.*

5. *Anschließend geben Sie im Feld FREIGABENAME den Freigabenamen ein. Verwenden Sie ggf. den Namen des Ordners.*

6. *Klicken Sie auf WEITER, um im nächsten Fenster die Berechtigungen zuzuweisen.*

7. *Sobald Sie den Vorgang mit FERTIGSTELLEN abgeschlossen haben, wird die Freigabe erstellt.*

8.3 NTFS-Berechtigungen

NTFS-Berechtigungen gewähren oder verweigern Benutzern den Zugriff auf Dateien und/oder Ordner. Sie sind im Gegensatz zu den Freigabeberechtigungen nur verfügbar, wenn der Datenträger mit dem Dateisystem **NTFS** eingerichtet wurde. Die Berechtigungen werden ähnlich wie bei den Freigabeberechtigungen den Benutzer- bzw. Gruppenkonten zugewiesen. Die NTFS-Berechtigungen sind wirksam, wenn lokal oder über das Netzwerk auf einen Ordner oder eine Datei zugegriffen wird.

Administratoren und die **Besitzer einer Datei oder eines Ordners** können Berechtigungen zuweisen.

Folgendes sollte bei der Administration von NTFS-Berechtigungen berücksichtigt werden:

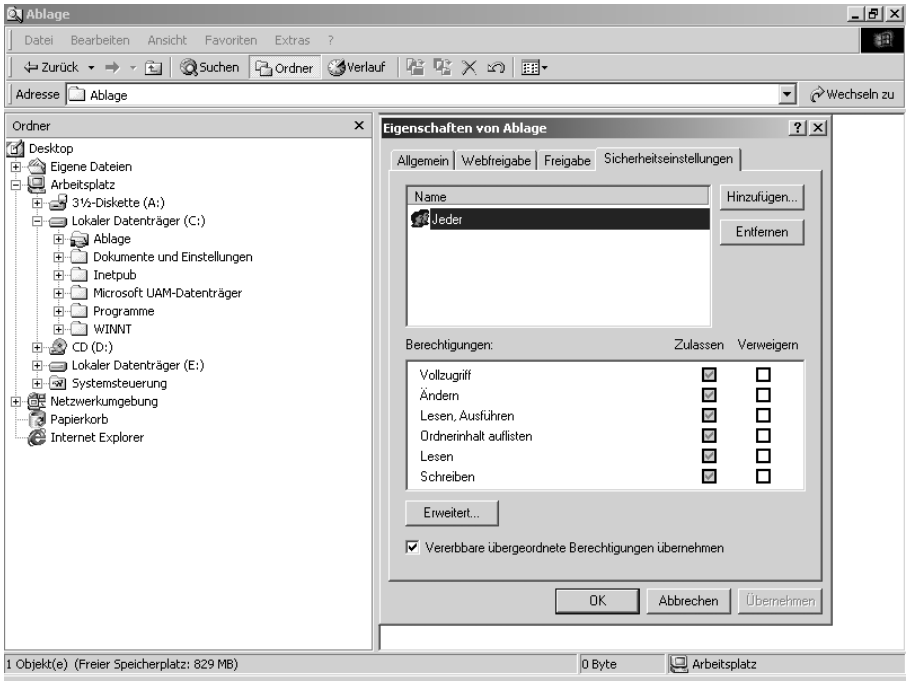
- *Verwenden Sie NTFS-Berechtigungen zum Steuern des Datei- und Ordnerzugriffs. Ermitteln Sie, welche Gruppen Zugriff auf welche Ressourcen haben müssen und welche Zugriffsebene erforderlich ist.*

- *Weisen Sie die Berechtigungen nur Gruppen- und nicht Benutzerkonten zu, um die Zugriffsverwaltung einfacher zu gestalten.*

- *Geben Sie den Benutzer- und Gruppenkonten keine Vollzugriffsrechte. Entfernen Sie beim Zuweisen von Berechtigungen die standardmäßige Gruppe Jeder mit der Berechtigung Vollzugriff.*

- *Weisen Sie das Mindestmaß an erforderlichen Berechtigungen zu. Dadurch wird das Risiko verringert, dass Benutzer versehentlich Dokumente und Anwendungsdateien ändern oder löschen.*

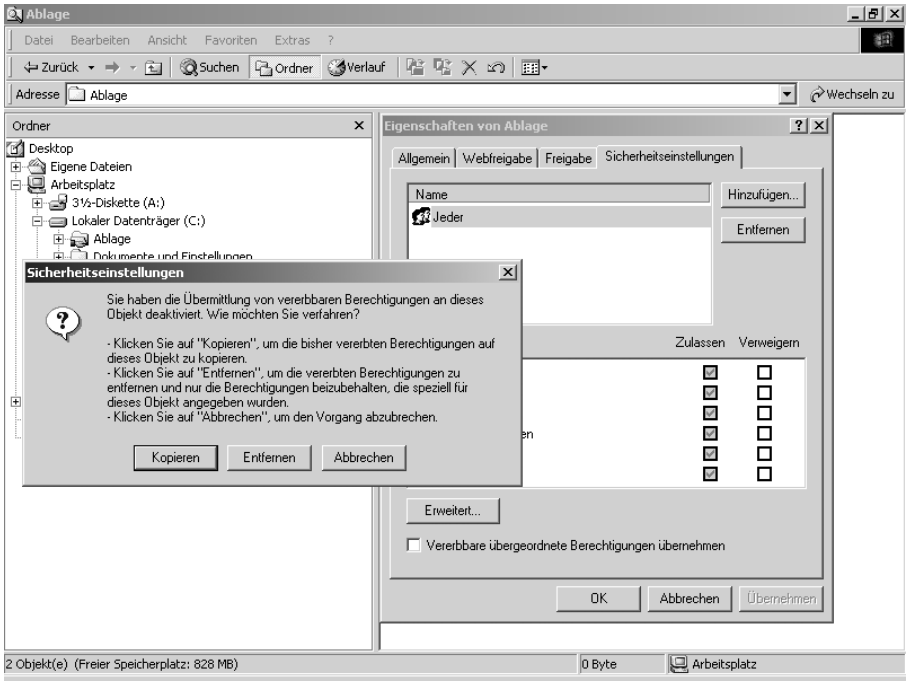
- *Dokumentieren Sie die Gruppen und ihre Berechtigungen für jede Ressource.*



NTFS-Berechtigungen, Ordner „Ablage“

Option	**Beschreibung**
Name	Dieses Feld listet die Benutzer- und Gruppenkonten mit Berechtigungen für die Datei oder den Ordner auf.
Berechtigungen	In diesem Feld können einem Benutzer- oder Gruppenkonto Berechtigungen zugewiesen werden.
Hinzufügen	Über HINZUFÜGEN können Benutzer- oder Gruppenkonten ausgewählt werden, die Berechtigungen erhalten sollen.
Entfernen	Über ENTFERNEN können Benutzer- oder Gruppenkonten die Berechtigungen für den Ordner oder die Datei entzogen werden.
Vererbbare übergeordnete Berechtigungen übernehmen	Ist diese Option aktiviert, werden die Berechtigungen automatisch von dem übergeordneten Ordner auf die untergeordneten Ordner und Dateien übernommen. Standardmäßig ist diese Option immer aktiv.
Erweitert	Die Schaltfläche ERWEITERT öffnet das Dialogfeld ZUGRIFFSEINSTELLUNGEN. Dort können detaillierte NTFS-Zugriffsberechtigungen, Überwachungsfunktionen und die Besitzübernahme administriert werden.

Standardmäßig werden die zugewiesenen Berechtigungen eines übergeordneten Ordners an die Unterordner und die in ihm enthaltenen Dateien vererbt, die Kontrollkästchen der Berechtigungen werden in diesem Fall grau hinterlegt dargestellt. Dadurch wird die Administration der NTFS-Berechtigungen erheblich vereinfacht. Erst nachdem die Option VERERBBARE ÜBERGEORDNETE BERECHTIGUNGEN ÜBERNEHMEN deaktiviert wird, besteht die Möglichkeit, entweder die vererbten Berechtigungen zu kopieren oder sie insgesamt zu entfernen (siehe Abbildung).

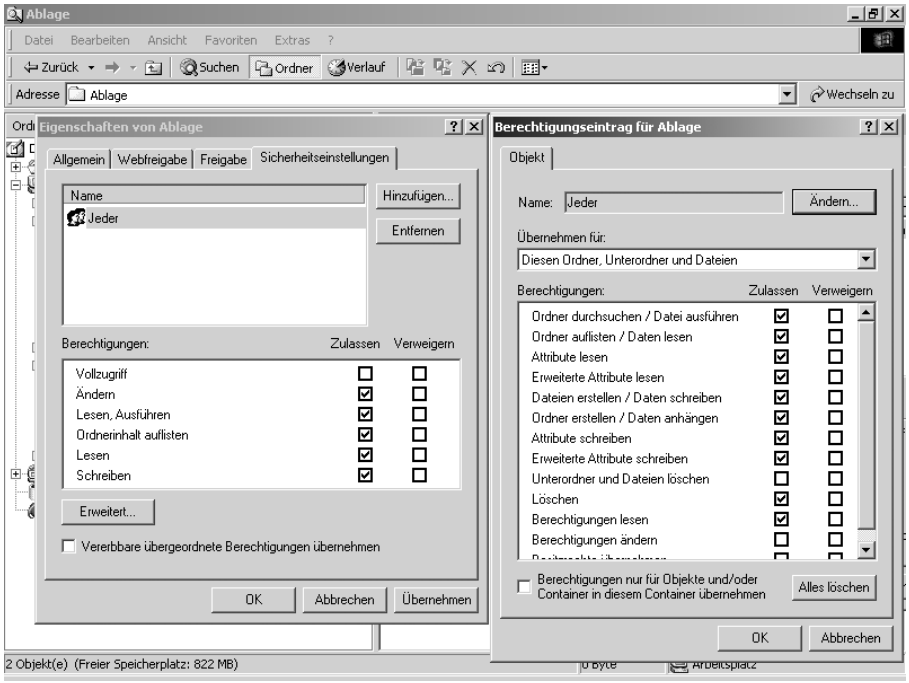


NTFS-Berechtigungen, Vererbung deaktivieren

Mit der Standardinstallation von Windows 2000 wird einem Laufwerk (z. B. C:\ oder D:\) automatisch die Gruppe *Jeder* mit *Vollzugriff* zugewiesen. Deshalb sollten zunächst die NTFS-Berechtigungen der eingerichteten Laufwerke (z. B. C:\, D:\) überprüft und ggf. geändert werden.

- Wird ein Ordner auf oberster Ebene (z. B. C:\) angelegt, erbt er die Berechtigung des Festplattenlaufwerkes bzw. Datenträgers.
- Ändert der Administrator die Berechtigung eines Ordners, so werden diese Änderungen automatisch auf alle Unterordner vererbt.
- Vererbte Berechtigungen werden grau schattiert angezeigt.

Die Berechtigungsvergabe kann sehr differenziert durchgeführt werden. Häufig auftretende Standardberechtigungen können mithilfe von vorgegebenen Schablonen vergeben werden, die mehrere einzelne NTFS-Berechtigungen zusammenfassen (siehe Tabelle). Über die Funktion ERWEITERT lassen sich die einzelnen NTFS-Detailberechtigungen aber auch differenziert zuweisen.



Detaillierte NTFS-Berechtigungen

Detailberechtigungen	**Schablonenberechtigungen**					
	Voll-zugriff	**Ändern**	**Lesen, Ausführen**	**Ordner-inhalt auflisten**	**Lesen**	**Schreiben**
Ordner durchsuchen/Datei ausführen	×	×	×	×		
Ordner auflisten/Daten lesen	×	×	×	×	×	
Attribute lesen	×	×	×	×	×	
Erweiterte Attribute lesen	×	×	×	×	×	
Dateien erstellen/Daten schreiben	×	×				×
Ordner erstellen/Daten anhängen	×	×				×
Attribute schreiben	×	×				×

Erweiterte Attribute schreiben	×	×				×
Unterordner und Dateien löschen	×					
Löschen	×	×				
Berechtigungen lesen	×	×	×	×	×	
Berechtigungen ändern	×	×				
Besitzrechte übernehmen	×					

- Sie können auch gleichzeitig mehrere Schablonen aktivieren, z. B. *Lesen* und *Schreiben*.
- Um nachvollziehbare Berechtigungsstrukturen zu erhalten, sollten Sie die Vergabe von Detailberechtigungen nur dort anwenden, wo der Benutzer Zugriff auf die Ordner- und Dateiebene, wie z. B. Word, erhält.
- Entziehen Sie dem Benutzer grundsätzlich die NTFS-Detailberechtigungen BERECHTIGUNGEN ÄNDERN und BESITZ ÜBERNEHMEN. Diese Rechte sollten nur von dem Administrator ausgeübt werden dürfen.

In dem Feld ÜBERNEHMEN FÜR kann darüber hinaus ausgewählt werden, welchen Objekten (Ordner, Dateien) Berechtigungen zugewiesen werden sollen. Folgende Objektzuweisungen sind möglich:

Option	**Beschreibung**
Nur diesen Ordner	Die Berechtigungen werden ausschließlich nur dem ausgewählten Ordner zugewiesen. Unterordner und Dateien werden nicht in die Berechtigungszuweisung einbezogen.
Diesen Ordner, Unterordner und Dateien	Die Berechtigungen werden dem ausgewählten Ordner und allen Dateien und Unterordnern zugewiesen.
Diesen Ordner, Unterordner	Die in dem Ordner enthaltenen Dateien erhalten die erteilten Berechtigungen nicht.

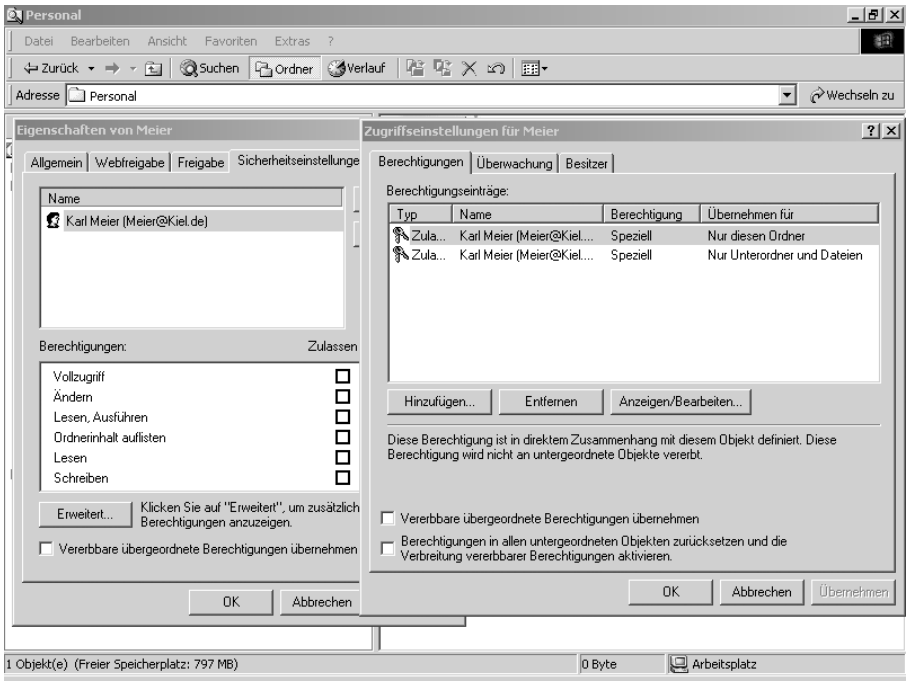
Diesen Ordner, Dateien	Die Unterordner werden in die Berechtigungszuweisung nicht mit einbezogen.
Nur Unterordner und Dateien	Die Berechtigungen werden nur den Unterordnern und den Dateien zugewiesen.
Nur Unterordner	Die Berechtigungen werden nur den Unterordnern ohne Einbeziehung der Dateien zugewiesen.
Nur Dateien	Die Berechtigungen werden nur den Dateien zugewiesen.

Die Administration der zugewiesenen Berechtigungen kann sehr differenziert durchgeführt werden. Aufgrund einer fehlerhaften Rechtezuweisung können Situationen entstehen, in denen Benutzer mehr Zugriffsmöglichkeiten erhalten als ursprünglich vorgegeben. Sie sollten deshalb stets unter dem entsprechenden Benutzerkonto die Rechtezuweisungen überprüfen.

NTFS-Berechtigungen einem Benutzerkonto zuweisen!

1. *Klicken Sie mit der rechten Maustaste auf einen Ordner, für den Sie NTFS-Berechtigungen vergeben möchten.*
2. *Klicken Sie auf EIGENSCHAFTEN und danach wählen Sie die Registerkarte SICHERHEITSEINSTELLUNGEN.*
3. *Deaktivieren Sie die Option VERERBBARE ÜBERGEORDNETE BERECHTIGUNGEN ÜBERNEHMEN und klicken Sie danach auf ENTFERNEN.*
4. *Klicken Sie auf HINZUFÜGEN, um aus der Liste der Benutzer- und Gruppenkonten ein Benutzerkonto durch einen Doppelklick auszuwählen. Bestätigen Sie mit OK.*
5. *Wählen Sie nun unter ZULASSEN die gewünschte Schablonenberechtigung (z. B. Ändern) aus.*
6. *Klicken Sie auf OK, um die Berechtigungen zu übernehmen.*

Ist auf dem Server eine **zentrale Datenablage** für die Speicherung von z. B. Worddateien eingerichtet, ist zu beachten, dass die vorgegebene Ablagestruktur nicht von den Benutzern verändert werden kann. In diesem Fall ist die Vergabe von Detailberechtigungen notwendig, um die Ablagestrukturen vor unerwünschten Veränderungen zu schützen.



Detaillierte Zugriffsberechtigungen des Ordners „Meier“

Die vor Veränderungen der Benutzer zu **schützenden Ordner** dürfen keine Löschungs- und Besitzübernahmeberechtigungen enthalten. Erst auf der **letzten** zu schützenden Ordnerebene, unter der der Benutzer selbst verantwortlich für die Verwaltung „seiner Unterordner und Dateien“ ist, kann zusätzlich die Löschberechtigung zugewiesen werden. Des Weiteren sollte überprüft werden, ob der Zugriff der Administratorkonten auf Ordner mit Worddateien notwendig ist.

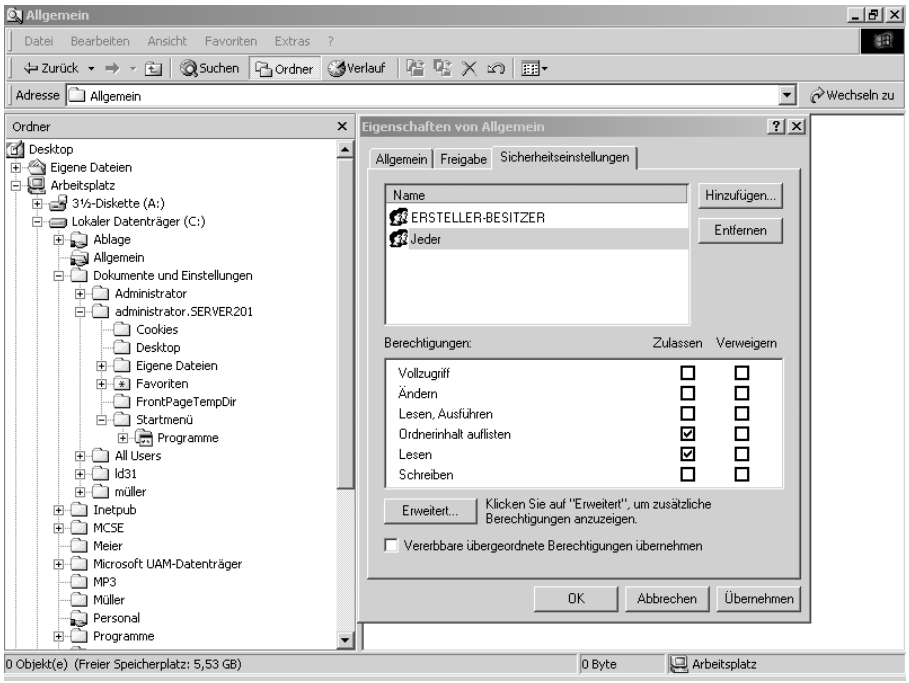
Die folgende Tabelle zeigt die Zuweisung von NTFS-Berechtigungen am Beispiel einer zentralen Ablage. Jeder Mitarbeiter darf die Struktur der Ablage sehen, aber nicht verändern oder Ordner löschen. Der Administrator darf die Struktur der Ablage vollständig administrieren, soll aber keinen Zugriff auf die Ordner der Benutzer erhalten. Jeder Benutzer, hier am Beispiel des Benutzers Meier, darf „seinen“ (vom Administrator angelegten) Ordner nicht löschen. Er erhält aber die Berechtigung in „seinem“ Ordner Unterordner und Dateien anlegen.

Ordnerstruktur	**Ordnerebene**					
C:\Zentrale Ablage\Personal\Meier	Zentrale Ablage		Personal		Meier	
Benutzer- und Gruppenkonten	Administratoren	Jeder	Administratoren	Personal	Meier	Meier
Übernehmen für	diesen Ordner, Unterordner und Dateien	diesen Ordner	diesen Ordner, Unterordner und Dateien	diesen Ordner	nur diesen Ordner	nur Unterordner und Dateien
Detailberechtigungen						
Ordner durchsuchen/Datei ausführen	×		×		×	×
Ordner auflisten/Daten lesen	×	×	×	×	×	×
Attribute lesen	×		×		×	×
Erweiterte Attribute lesen	×		×		×	×
Dateien erstellen/Daten schreiben	×		×		×	×
Ordner erstellen/Daten anhängen	×		×		×	×
Attribute schreiben	×		×		×	×
Erweiterte Attribute schreiben	×		×		×	×
Unterordner und Dateien löschen	×		×		×	×
Löschen	×		×			×
Berechtigungen lesen	×		×			
Berechtigungen ändern	×		×			
Besitzrechte übernehmen	×		×			

Des Weiteren ist bei der Einrichtung einer zentralen Ablage die spezielle Gruppe ERSTELLER-BESITZER von Bedeutung. Die Gruppe kann als so genannter Platzhalter verwendet werden. Wenn z. B. mehrere Benutzer auf einen **allgemeinen Ordner** lesend und schreibend zugreifen sollen, besteht die Gefahr, dass ein Benutzer die Datei eines anderen unberechtigterweise

verändert. Es müssen demnach Berechtigungen vergeben werden, unter denen der Benutzer seine „eigenen“ Dateien lesend und schreibend und die Dateien anderer Benutzer ausschließlich im lesenden Zugriff bearbeiten kann.

Würde es die Gruppe ERSTELLER-BESITZER nicht geben, könnten diese Anforderungen nicht umgesetzt werden, weil mit dem Entzug der Schreibberechtigung das Erstellen der Dateien im Ordner nicht mehr möglich wäre.



Explorer, Gruppe ERSTELLER-BESITZER

Wird dem Ordner allerdings die Gruppe ERSTELLER-BESITZER mit Schreibleseberechtigungen zugewiesen, dann werden automatisch dem **entsprechenden Benutzer**, der innerhalb dieses Ordners Unterordner oder Dateien anlegt, Zugriffsrechte auf „seine“ Objekte gewährt.

Legt Benutzer A beispielsweise eine Datei in einen allgemeinen Ordner mit der Gruppe ERSTELLER-BESITZER ab, werden der Datei zunächst die Berechtigungen des allgemeinen Ordners übertragen (in der Abbildung die Gruppe JEDER mit Lesezugriff). Zusätzlich wird aber der Datei automatisch das Benutzerkonto von A mit den Berechtigungen der übergeordneten Gruppe ERSTELLER-BESITZER zugewiesen. Somit ist sichergestellt, dass die Benutzer auf ihre Dateien uneingeschränkt und auf die Dateien anderer Benutzer nur eingeschränkt zugreifen können.

- Wenn Sie einem Ordner **mehrere** Gruppenkonten mit unterschiedlichen Berechtigungen zuweisen, in denen dasselbe Benutzerkonto Mitglied ist, dann erhält es das höchste Recht.

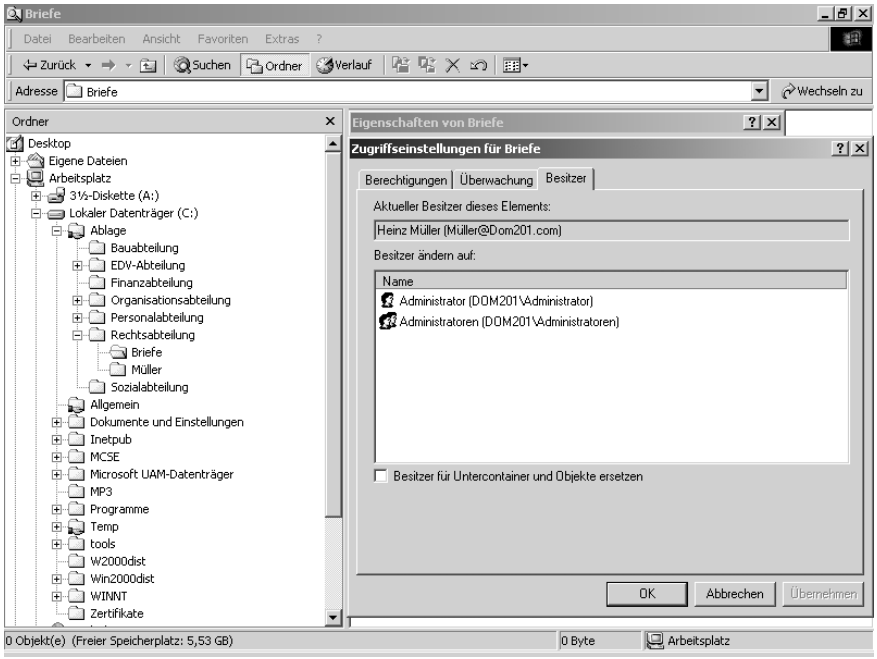
- Dateiberechtigungen werden **vor** Ordnerberechtigungen umgesetzt. Wenn z. B. ein Benutzer Schreibleseberechtigungen auf eine Datei und nur Leseberechtigungen auf einen Ordner erhält, überwiegen die Dateiberechtigungen.

- Bei der **Kombination** von Freigabeberechtigungen und NTFS-Berechtigungen wird die Berechtigung mit der größten Einschränkung berücksichtigt.

- Das **Verweigern** von NTFS-Berechtigungen ist wie bei den Freigabeberechtigungen anzuwenden. Wenn Sie einer Gruppe Zugriffsrechte erteilt haben, können Sie einem einzelnen Benutzerkonto, das Mitglied dieser Gruppe ist, die Berechtigungen unter VERWEIGERN entziehen. Verweigerte NTFS-Berechtigungen werden vorrangig berücksichtigt.

8.4 Besitzübernahme von Ordnern und Dateien

Standardmäßig ist der **Ersteller** eines Ordners oder einer Datei der Besitzer. Er erhält automatisch Vollzugriff und bekommt das Recht, die NTFS-Berechtigungen für „seine“ Ordner und Dateien zu administrieren.

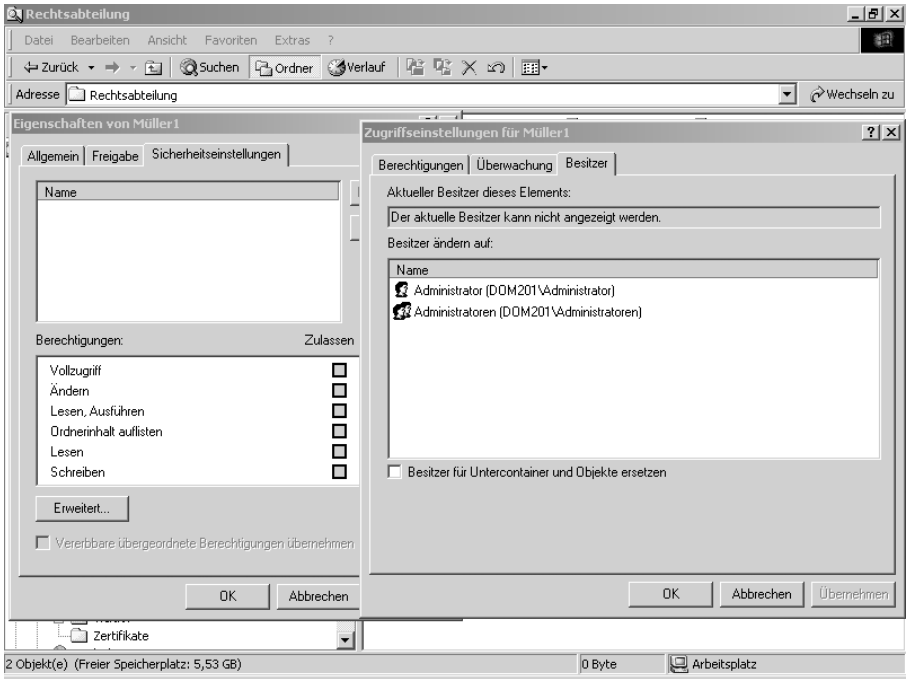


Zugriffseinstellungen für den Ordner „Briefe“

Damit kann er selbst bestimmen, welche Benutzer und Administratoren auf „seine“ Ordner und Dateien zugreifen dürfen. Diese Rechte sollte jedoch ein Benutzer ausschließlich nur in „seinem“ Ordner der Dokumentenablage erhalten, da er sonst die Zugriffsberechtigungen „fremder“ Ordner und Dateien beliebig verändern könnte. Die Datensicherheit wäre somit nicht mehr gewährleistet.

Die Mitglieder der Gruppe ADMINISTRATOREN haben immer die Möglichkeit, den Besitz an einem Ordner oder an einer Datei zu übernehmen. Sie können aber mit den Funktionen von Windows 2000 den Besitz **nicht** auf andere übertragen.

Um **sensible Daten** in einer Dokumentenablage vor dem Zugriff der Administration zu schützen, wird empfohlen, die entsprechenden Ordner von den Benutzern selbst anlegen zu lassen. Sie werden dann Besitzer der Ordner und können die NTFS-Berechtigungen selbst administrieren. Den Administratoren kann auf diese Weise der Zugriff auf die Ordner entzogen werden. Sie haben nur die Möglichkeit, den Besitz des Ordners zu übernehmen, um sich Zugriff zu verschaffen. Dieser Vorgang hinterlässt jedoch „**Spuren**“, denn sie können den Besitz nicht auf den vorherigen Besitzer zurückübertragen. Durch eine regelmäßige Überprüfung der Besitzereinstellungen können somit Manipulationen in Bezug auf die Zugriffsberechtigungen durch die Administration erkannt werden.



Besitzübernahme durch den Administrator

Besitz eines Ordners übernehmen!

1. *Klicken Sie mit der rechten Maustaste auf den Ordner, dessen Besitz Sie übernehmen möchten.*
2. *Klicken Sie auf* EIGENSCHAFTEN *und danach wählen Sie die Registerkarte* SICHERHEITSEINSTELLUNGEN.
3. *Klicken Sie auf die Option* ERWEITERT *und danach auf die Registerkarte* BESITZER.
4. *In dem Dialogfeld* BESITZER ÄNDERN AUF *wird standardmäßig das Benutzerkonto* ADMINISTRATOR *und das Gruppenkonto* ADMINISTRATOREN *angezeigt.*
5. *Wählen Sie das Gruppenkonto* ADMINISTRATOREN *und klicken Sie auf die Option* ÜBERNEHMEN. *Der Besitz wird nun übernommen. Dabei bleiben die für den Ordner vergebenen NTFS-Berechtigungen erhalten.*
6. *Ändern Sie ggf. die NTFS-Berechtigungen, sofern dies erforderlich ist.*

- Mit der Besitzübernahme eines Ordners oder einer Datei werden die dem Ordner zugeordneten NTFS-Berechtigungen im Gegensatz zu Windows NT 4.0 nicht gelöscht.
- Den Benutzern/Administratoren wird der Besitzer nur angezeigt, wenn sie über lesende Zugriffsrechte auf den Ordner oder die Datei verfügen.

- Einen beabsichtigten Zugriff auf personenbezogene Daten durch **Administratoren** werden Sie mit technischen Sicherheitsmaßnahmen nur schwer verhindern können. Es gibt viele Hacker-Tools (z. B. *setowner* <www.ntsecurity.nu>), mit denen Sicherheitsmaßnahmen ausgehebelt werden können.
- Des Weiteren ist der Zugriff auf personenbezogene Daten über die Datensicherungsbänder nicht zu unterschätzen. Diese könnten z. B. zu Hause in aller Ruhe missbraucht werden.
- Geplante und mit Aufwand verbundene unberechtigte Zugriffe auf personenbezogene Daten haben allerdings eine andere „Qualität“ als ein einfacher, ungehinderter Zugriff auf personenbezogene Daten.

8.5 Kopieren und Verschieben von Ordnern und Dateien

Zum **Kopieren** von Dateien und Ordnern innerhalb oder zwischen NTFS-Datenträgern muss ein Benutzer für den Zielordner mindestens über die Berechtigung DATEIEN ERSTELLEN/DATEN SCHREIBEN und ORDNER ERSTELLEN/DATEN ANHÄNGEN verfügen. Der Benutzer, der den Kopiervorgang durchführt, wird zum Besitzer der neuen Datei oder des neuen Ordners im Zielordner.

Das **Verschieben** von Dateien und Ordnern zwischen NTFS-Partitionen erfordert für den **Zielordner** die Berechtigungen DATEIEN ERSTELLEN/DATEN SCHREIBEN, ORDNER ERSTELLEN/DATEN ANHÄNGEN. Darüber hinaus werden für den **Quellordner** mindestens die Berechtigungen ORDNER AUFLISTEN/DATEN LESEN und LÖSCHEN benötigt. Die Berechtigung LÖSCHEN wird zum Verschieben eines Ordners oder ein Datei benötigt, da der Ordner oder die Datei aus dem Quellverzeichnis gelöscht wird, nachdem sie in den Zielordner verschoben wurde.

Folgende Regeln sind beim Kopieren und Verschieben zu beachten:

- Die Freigabeberechtigungen eines Ordners werden beim Kopieren oder Verschieben aufgehoben.

- Werden Dateien oder Ordner auf Datenträger kopiert oder verschoben, die nicht das NTFS-Dateisystem unterstützen (z. B. Disketten), **verlieren** die Ordner und Dateien ihre NTFS-Berechtigungen.

- Wird ein Ordner oder eine Datei innerhalb einer NTFS-Partition **kopiert**, **erbt** der Ordner oder die Datei die NTFS-Berechtigungen des Zielordners.

- Werden Dateien oder Ordner auf demselben NTFS-Datenträger verschoben, behalten sie ihre ursprünglichen NTFS-Berechtigungen.

- Bei einem Verschieben auf einen anderen NTFS-Datenträger übernimmt der Ordner oder die Datei die NTFS-Berechtigungen des Zielordners. Der Benutzer, der den Vorgang des Verschiebens durchführt, wird zum ERSTELLER-BESITZER der entsprechenden Ordner und Dateien.

8.6 Verschlüsselung von Ordnern und Dateien

Mit dem EFS **(Encrypting File System)** verfügen die Benutzer über die Funktion, Ordner und Dateien zu verschlüsseln. Dieses Recht ist nicht Bestandteil der NTFS-Berechtigungen, sondern kann für einen Ordner oder eine Datei gezielt aktiviert werden. Nach Markierung mit der rechten Maustaste kann ein Benutzer mit der Option EIGENSCHAFTEN-ERWEITERT-INHALT VERSCHLÜSSELN einen Ordner oder eine Datei verschlüsseln. Öffnet er den Ordner bzw. die Datei erneut, so wird sie automatisch entschlüsselt.

Verschlüsselungsverfahren

EFS wird genutzt für die

- Verschlüsselung der Datei und die
- Verschlüsselung des Schlüssels, mit dem die Datei verschlüsselt wird.

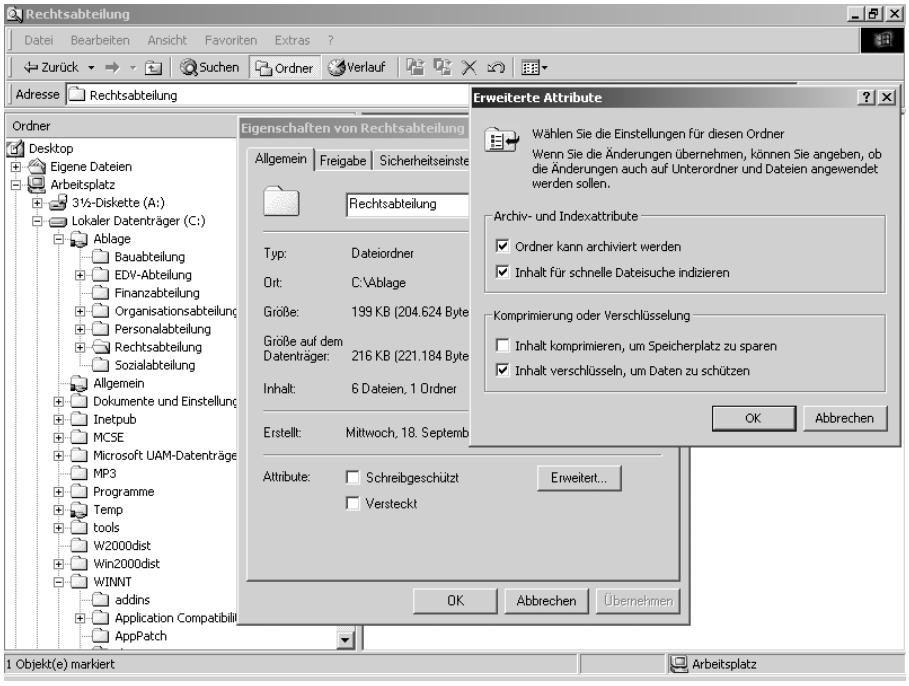
EFS verschlüsselt die Dateien mit dem erweiterten *US Data Encryption Standard* (DESX). Dabei wird die Datei in einer 3-stufigen Kombination verschlüsselt. Es wird vom EFS eine Zufallszahl erzeugt, die als DESX-Schlüssel verwendet wird. Diese Zufallszahl heißt *File Encrypting Key* (FEK). Vom FEK stehen eine 128-Bit- und eine 56-Bit-Version zur Verfügung, standardmäßig ist die 56-Bit-Version installiert. Der DESX-Algorithmus ist symmetrisch, d. h. ein Schlüssel wird sowohl zur Verschlüsselung als auch zur Entschlüsselung benutzt. Der zur Dateientschlüsselung nötige Schlüssel (FEK) wird nicht in einem lesbaren Format gespeichert, sondern durch eine Verschlüsselung anhand der *Public Key Cryptography System-Technologie* (PKCS) geschützt.

PKCS ist nicht symmetrisch, d. h. statt eines Schlüssels zur Ver- und Entschlüsselung wird zur Verschlüsselung des FEK die Technologie des Paares öffentlicher/privater Schlüssel verwendet. Der öffentliche Schlüssel wird zur Verschlüsselung, der private Schlüssel zur Entschlüsselung eingesetzt. Der private Schlüssel ist an das Anmeldekennwort des Benutzers gekoppelt. Der öffentliche Schlüssel lässt sich frei verteilen. Dateien, die mit dem öffentlichen Schlüssel verschlüsselt werden, sind so lange sicher, solange keiner außer dem Besitzer Zugriff auf den privaten Schlüssel hat.

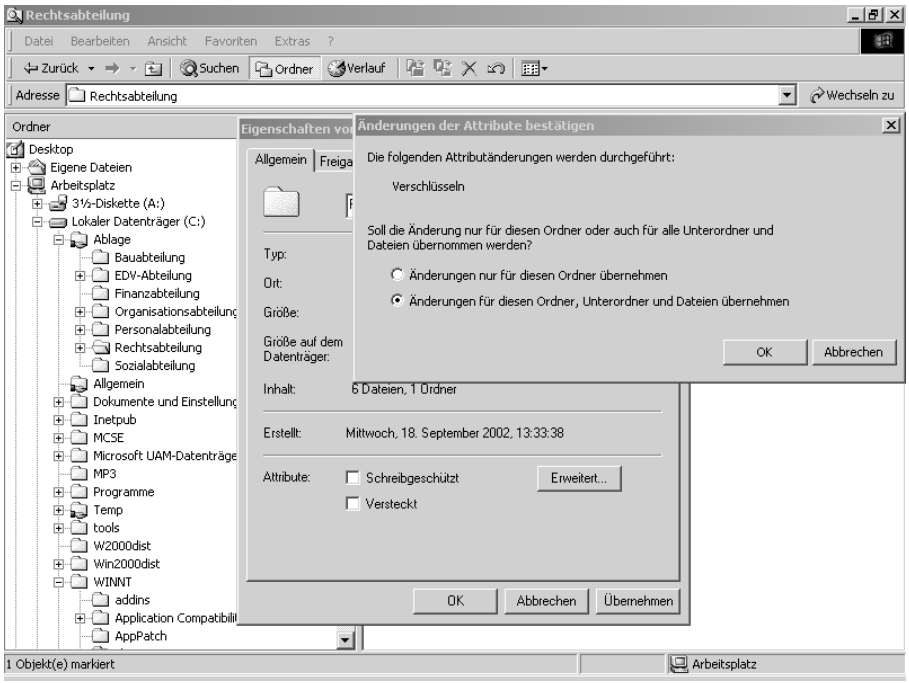
Der Dienst, mit dem EFS-Zertifikate ausgestellt werden, heißt Microsoft Base Crytographic Provider v 1.0.

Für die Aktivierung der Verschlüsselung benötigt der Benutzer mindestens Lese- und Schreibberechtigungen auf den Ordner oder die Datei. Sofern die Verschlüsselung auf Ordnerebene aktiviert wird, können alle in dem Ordner enthaltenen Unterordner und Dateien in einem Zuge mit verschlüsselt werden.

Die Verschlüsselung von Daten ist insbesondere dann zu aktivieren, wenn **mobile PC** verwendet werden. Im Einzelfall kann aber auch auf den internen Systemen die Verschlüsselung eingesetzt werden, wenn personenbezogene Daten vor **administrativen Zugriffen** zu schützen sind. Das erfordert jedoch **umfangreiche Kenntnisse** über den richtigen Einsatz des Verschlüsselungsverfahrens.



Eigenschaften – Erweiterte Attribute zum Verschlüsseln eines Ordners

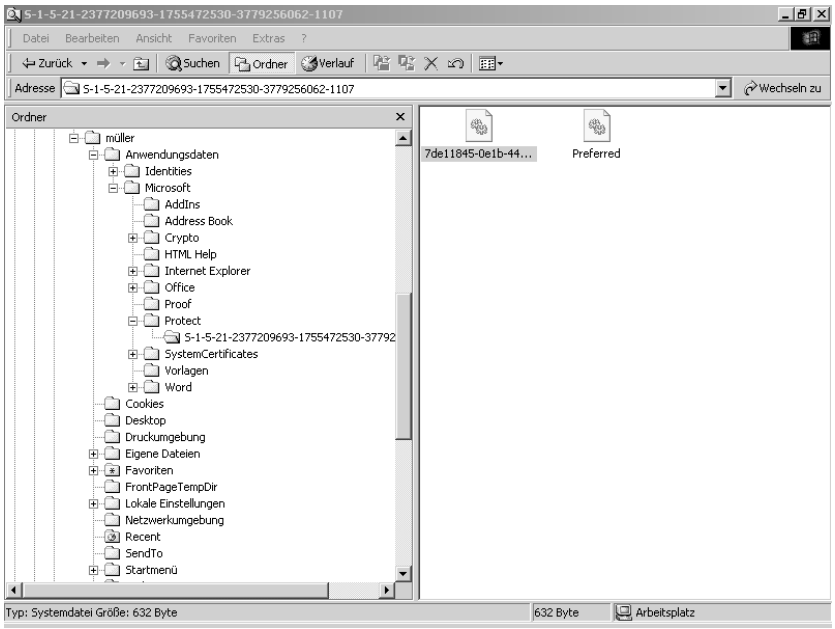


Verschlüsselung eines Ordners unter Einbeziehung aller Unterordner und Dateien

Aus Sicherheitsgründen ist unter Windows 2000 standardmäßig ein so genannter **Datenwiederherstellungsagent** (Data Recovery Agent, DRA) eingerichtet, der auf alle verschlüsselten Ordner und Dateien der Benutzer zugreifen kann. Ist beispielsweise ein Benutzer nicht anwesend, kann der Datenwiederherstellungsagent die verschlüsselten Ordner und Dateien des entsprechenden Benutzers entschlüsseln. Der Zugriff ist somit „abgesichert“. Die Funktion des Datenwiederherstellungsagenten ist dem Administratorkonto zugeordnet.

Betriebssystem/Serverfunktion	**Standard-DRA-Benutzerkonto**
Windows 2000 Professional-Desktop	Lokales Administratorkonto (SAM)
Windows 2000 Server (Mitgliedserver)	Lokales Administratorkonto (SAM)
Windows 2000 Domänencontroller	Active Directory-Administratorkonto

Verschlüsselt ein Benutzer einen Ordner oder eine Datei das erste Mal, dann wird ein Paar **öffentlicher/privater Schlüssel** erzeugt. Der öffentliche und der private Schlüssel werden als Dateien im **Benutzerprofil** des entsprechenden Benutzers gespeichert. Der **private Schlüssel** ist auf dem Datenträger im Pfad <C:\Dokumente und Einstellungen\<Benutzername>\Anwendungsdaten\Microsoft\Protect\<Benutzer-SID> gespeichert. Er wird benötigt, um die verschlüsselte Datei zu lesen. Der Schlüssel ist an das Kennwort des Benutzers gekoppelt. Ändert der Benutzer das Kennwort, wird es an das neue Kennwort gekoppelt.



Explorer, privater Schlüssel

Beachten Sie, dass ein Benutzer, der über ein lokales Benutzerkonto Ordner oder Dateien verschlüsselt hat, diese nicht über sein Domänen-Benutzerkonto entschlüsseln kann. In diesem Fall handelt es sich zwar um denselben Benutzer, aber um zwei unterschiedliche Benutzerkonten/-profile, denen jeweils ein anderes Schlüsselpaar zugewiesen wurde.

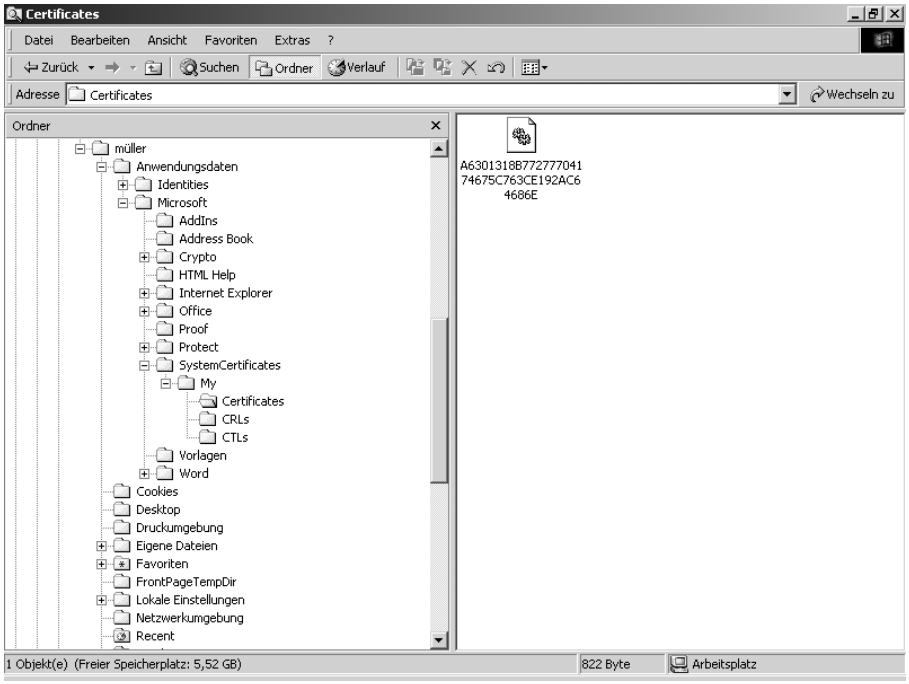
- Standardmäßig ist auf eine Vielzahl von Ordnern und Dateien die NTFS-Berechtigung ATTRIBUTE SCHREIBEN vergeben. Es besteht deshalb die Gefahr, dass Benutzer Ordner und Dateien des Betriebssystems und/oder anderer Benutzer (ungewollt) verschlüsseln können. Überprüfen Sie deshalb diesbezüglich die NTFS-Berechtigungen.

- Bevor Sie ein Benutzerkonto aus der Domäne entfernen, überprüfen Sie, ob zu diesem Benutzerkonto verschlüsselte Ordner oder Dateien vorliegen. Denn mit der Löschung des Benutzerkontos kann der im Benutzerprofil gespeicherte private Schlüssel nicht mehr verwendet werden.

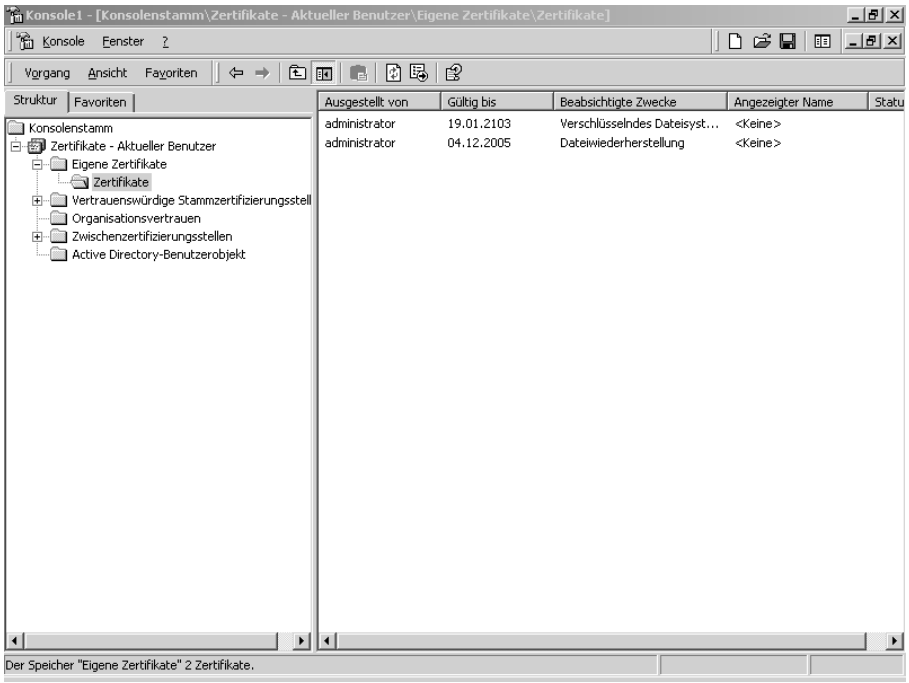
- Sofern Sie das Benutzerprofil eines Benutzerkontos löschen, ist ebenfalls der Zugriff auf verschlüsselte Ordner oder Dateien nicht mehr möglich, da nach dem Anmelden des Benutzers ein neues Benutzerprofil und ein neues Schlüsselpaar generiert werden. Der DRA kann jedoch noch in beiden Fällen die Dateien entschlüsseln.

Der **öffentliche Schlüssel** wird in Form eines Zertifikates gespeichert. Ein Zertifikat ist eine Datei, die den öffentlichen Schlüssel und weitere Elemente enthält, die die Authentizität des Schlüssels beglaubigen.

Das Zertifikat des öffentlichen Schlüssels ist auf dem Datenträger unter *<C:\Dokumente und Einstellungen\<Benutzername>\Anwendungsdaten\Microsoft\SystemCertificates\My\Certificates>* gespeichert. Der Dateiname, den das Zertifikat erhält, entspricht dem **Fingerabdruck** des Zertifikats (128-Bit), der eine schnelle Überprüfungsmöglichkeit der Identität des Zertifikats bietet (siehe Abbildung). Das Zertifikat des öffentlichen Schlüssels enthält den Benutzernamen der Person, die das Zertifikat besitzt, und damit auch den Hinweis, um den privaten Schlüssel des Benutzers finden zu können, wenn die Datei entschlüsselt werden muss. Jede verschlüsselte Datei ist mit einer Kopie des Zertifikats des öffentlichen Schlüssels versehen.



Explorer, öffentlicher Schlüssel



Snap-In Zertifikate – Aktueller Benutzer

Dem Datenwiederherstellungsagenten (DRA) ist ein Wiederherstellungszertifikat zugewiesen, das den öffentlichen und privaten Schlüssel dieses Agenten enthält. Wird eine Datei verschlüsselt, erhält der DRA eine Kopie des dazugehörigen *File Encrypting Key* (FEK), der mit dem öffentlichen Schlüssel aus dem Wiederherstellungszertifikat verschlüsselt und an die verschlüsselte Datei (Attribut $Logged_Utility_Stream) gekoppelt ist. Das gestattet es dem

DRA, die Datei auf dieselbe Weise zu öffnen wie der Benutzer, der die Datei verschlüsselt hat.

Das Zertifikat eines Benutzers (und dazu gehört auch der Administrator) ist mit dem Snap-In ZERTIFIKATE administrierbar. Dem Administratorkonto kann somit die Funktion des Datenwiederherstellungsagenten entzogen werden, indem das Wiederherstellungszertifikat durch das Exportieren auf eine Diskette entfernt wird. Dann besteht unter dem Administratorkonto nicht mehr die Möglichkeit, verschlüsselte Ordner und/oder Dateien zu entschlüsseln. Ein Importieren des Zertifikates wird erforderlich. Wenn die Diskette außerhalb der Verfügungsgewalt der Administration aufbewahrt wird, sind die verschlüsselten Daten der Benutzer vor einem administrativen Zugriff hinreichend geschützt.

Berücksichtigen Sie, dass die Fachverantwortlichen ebenfalls im Rahmen ihrer Kontrollpflichten nicht mehr direkt auf die verschlüsselten Datenbestände ihrer Mitarbeiter zugreifen können. Es bleibt nur der Weg über den Datenwiederherstellungsagenten.

Wiederherstellungszertifikat auf Diskette exportieren!

1. *Rufen Sie über START-AUSFÜHREN die MANAGEMENTKONSOLE auf, indem Sie* `mmc` *eingeben und mit OK bestätigen.*
2. *Klicken Sie auf das Menü KONSOLE und wählen Sie SNAP-IN HINZUFÜGEN/ENTFERNEN.*
3. *Klicken Sie auf HINZUFÜGEN und wählen Sie das Snap-In ZERTIFIKATE aus.*
4. *In dem Fenster ZERTIFIKAT-SNAP-IN aktivieren Sie die Option EIGENES BENUTZERKONTO. Klicken Sie dann auf FERTIGSTELLEN und danach auf OK. Das Snap-In ZERTIFIKATE ist nun in der Managementkonsole administrierbar.*
5. *Klicken Sie mit der linken Maustaste unter dem Konsolenstamm auf ZERTIFIKATE–AKTUELLER BENUTZER, danach auf EIGENE ZERTIFIKATE und dann auf ZERTIFIKATE.*
6. *Im rechten Fensterausschnitt werden zwei Zertifikate für die Verschlüsselung und Entschlüsselung angezeigt. Markieren Sie das Zertifikat mit der Beschreibung DATEIWIEDERHERSTELLUNG, indem Sie es mit der linken Maustaste anklicken, sodass es blau unterlegt ist.*

7. *Klicken Sie nun auf die rechte Maustaste und wählen Sie ALLE TASKS und danach EXPORTIEREN.*

8. *Folgen Sie den Anweisungen des Zertifikatsexport-Assistenten. Es ist ein Kennwort für den Schutz des Zertifikates einzugeben. Schreiben Sie sich das Kennwort auf und verwahren Sie es gut. Es ist für den Import des Zertifikates erforderlich. Speichern Sie die Zertifikatsdatei auf Diskette und beschriften Sie sie entsprechend.*

9. *Jetzt löschen Sie das im Snap-In exportierte Zertifikat, indem Sie mit der rechten Maustaste auf das Zertifikat klicken und LÖSCHEN wählen. Dem Administratorbenutzerkonto ist jetzt die Funktion des Datenwiederherstellungsagenten entzogen worden. Der Administrator ist nicht mehr in der Lage, die von Benutzern verschlüsselten Ordner und Dateien zu entschlüsseln.*

Wiederherstellungszertifikat von Diskette importieren!

1 .*Starten Sie die MANAGEMENTKONSOLE mit dem Snap-In ZERTIFIKATE.*

2. *Klicken Sie mit der linken Maustaste unter dem Konsolenstamm auf ZERTIFIKATE–AKTUELLER BENUTZER und danach auf EIGENE ZERTIFIKATE.*

3. *Mit der rechten Maustaste klicken Sie auf ZERTIFIKATE.*

4. *Wählen Sie ALLE TASKS und klicken Sie auf IMPORTIEREN. Es öffnet sich nun der Zertifikatsimport-Assistent.*

5. *Importieren Sie das auf der Diskette gespeicherte Zertifikat, indem Sie über DURCHSUCHEN das Diskettenlaufwerk und als Dateityp ALLE DATEIEN (*.*) auswählen.*

6. *Bestätigen Sie die weiteren Anweisungen des Assistenten. Geben Sie das entsprechende Kennwort ein, das Sie sich beim Exportieren gemerkt/notiert haben.*

7. *Das importierte Zertifikat muss ggf. noch unter dem Konsolenstamm in den Unterordner VERTRAUENSWÜRDIGE STAMMZERTIFIZIERUNGSSTELLEN–ZERTIFIKATE kopiert werden.*

8. *Klicken Sie mit der rechten Maustaste im Unterordner EIGENE ZERTIFIKAT– ZERTIFIKATE auf das zu kopierende Zertifikat und wählen Sie KOPIEREN.*

9. *Anschließend klicken Sie mit der rechten Maustaste auf den Unterordner VERTRAUENSWÜRDIGE STAMMZERTIFIZIERUNGSSTELLEN–ZERTIFIKATE und wählen EINFÜGEN.*

10. *Nach erfolgreichem Abschluss ist unter dem Administratorkonto nun wieder die Entschlüsselung der durch die Benutzer verschlüsselten Ordner und Dateien möglich.*

Folgende Regeln sind beim Einsatz der Verschlüsselung zu beachten:

- Unter dem Administratorkonto mit der Funktion des Datenwiederherstellungsagenten kann die von den Benutzern über das Attribut VERSCHLÜSSELUNG aktivierte Verschlüsselung jederzeit **deaktiviert** werden, sodass automatisch alle entsprechenden Ordner und Dateien entschlüsselt werden.

- Ein Benutzer kann die von einem anderen Benutzer verschlüsselten Ordner oder Dateien nicht entschlüsseln, indem er das Attribut VERSCHLÜSSELUNG deaktiviert.

- Beim Verschlüsseln von Dateien bleibt der Dateiname unberührt. Wenn ein Benutzer über die entsprechenden NTFS-Berechtigungen verfügt, kann er eine Datei umbenennen oder löschen, die von einem anderen Benutzer verschlüsselt wurde.

- Kopiert ein Benutzer eine von ihm verschlüsselte Datei auf einen FAT (FAT32)-Datenträger (Diskette), wird sie als entschlüsselte Textdatei gespeichert.

- Wird eine einzelne Datei verschlüsselt, erzeugt sie eine temporäre Datei. Die Datei Efs0.tmp wird ganz oder teilweise überschrieben, wenn die nächste Datei verschlüsselt wird. Sie hinterlässt jedoch möglicherweise Informationen, die ohne aufwendige Programme sichtbar gemacht werden können.

- Um eindeutige Strukturen zu erhalten, sollte die Verschlüsselung auf Ordnerebene aktiviert werden. Damit wird sichergestellt, dass alle Unterordner und Dateien automatisch verschlüsselt werden, ohne dass das Attribut VERSCHLÜSSELUNG erneut aktiviert werden muss. Das Verschlüsselungsattribut vererbt sich auf alle Unterordner und Dateien.

- Wenn ein Benutzer „seine“ Dateien in einen verschlüsselten Ordner eines anderen Benutzers speichert, werden sie mit dem öffentlichen Schlüssel des Benutzers verschlüsselt, der die Dateien erzeugt.

- Wird eine nicht verschlüsselte Datei in einen verschlüsselten Ordner kopiert oder verschoben, wird die Datei verschlüsselt.

- Werden verschlüsselte Dateien in nicht verschlüsselte Ordner verschoben oder kopiert, behalten sie ihren Status, wenn der Zieldatenträger mit NTFS-5 formatiert ist.

- Benutzerzertifikate werden im lokalen Benutzerprofil gespeichert. Werden Benutzerprofile gelöscht, kann nur der Dateiwiederherstellungsagent (DRA) die Dateien wiederherstellen. Wird das Zertifikat oder das Benutzerprofil des DRA gelöscht, können die Dateien endgültig nicht mehr entschlüsselt werden.

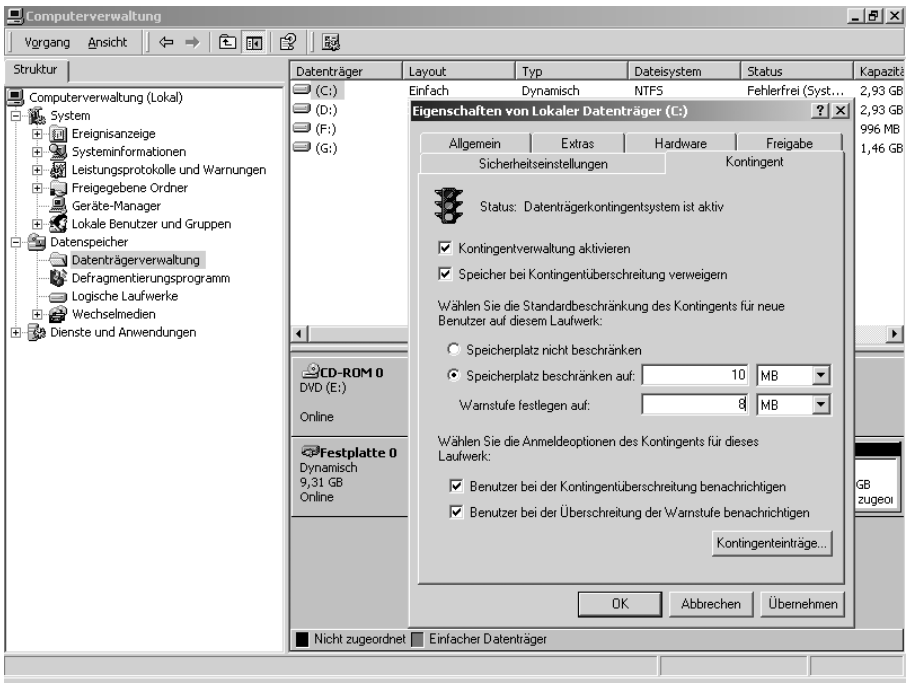
- Komprimierte Dateien lassen sich nicht verschlüsseln, und verschlüsselte Dateien können nicht komprimiert werden.
- Systemdateien lassen sich nicht verschlüsseln.

8.7 Datenträgerkontingente

Um zu verhindern, dass Benutzer auf dem Server oder Client übermäßig viele Daten speichern, oder um veraltete Daten zu löschen, können unter Windows 2000 **Datenträgerkontingente** vergeben werden. Die Einrichtung von Datenträgerkontingenten ist nur auf NTFS-5-Partitionen möglich.

Die Kontingente können benutzerbezogen auf jedem logischen Laufwerk getrennt eingerichtet werden. Sie sind unabhängig davon, in welchem Verzeichnis bzw. Ordner der Benutzer seine Daten speichert. Dabei spielt es keine Rolle, ob einzelne Laufwerke (z. B. G:\ oder H:\) physikalisch auf der gleichen Festplatte oder auf unterschiedlichen Festplatten liegen.

Wenn ein Benutzer eine Datei auf einen kontingentüberwachten NTFS-Datenträger kopiert, eine neue Datei erstellt oder das Besitzrecht an einer Datei übernimmt, wird die Kapazität dieser Datei auf sein Kontingent angerechnet.



Eigenschaften Datenträgerkontingente

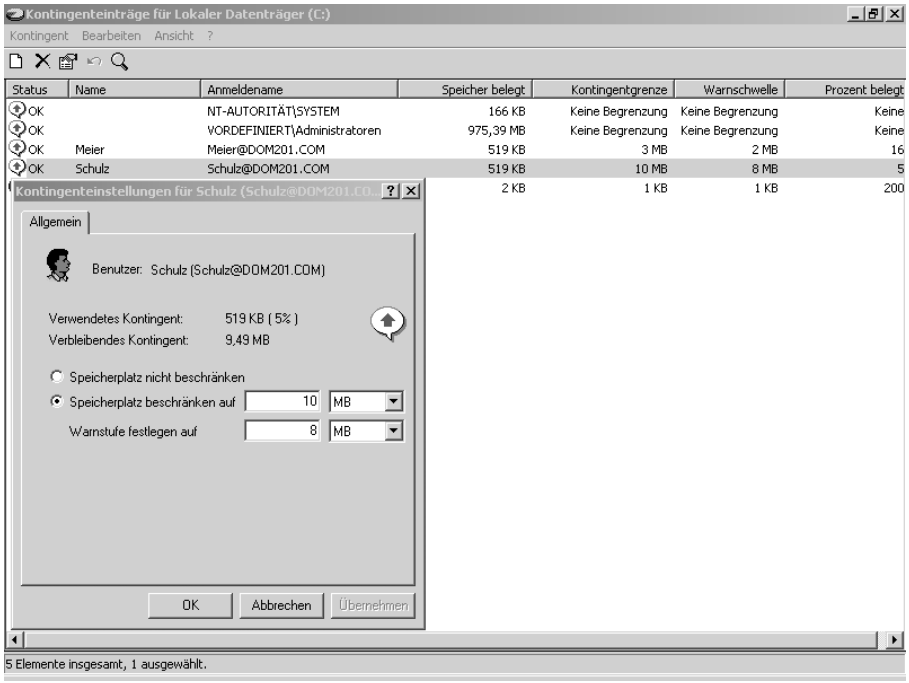
Einem Benutzer, der sein Kontingent überschritten hat, kann automatisch der weitere Zugang verwehrt werden. Kontingente können allgemein oder für spezielle Benutzer definiert werden. Die Administratoren werden bei einer allgemeinen Einrichtung nicht mit einbezogen.

Die Datenträgerkontingente werden in der Computerverwaltung über das Snap-In DATENTRÄGERVERWALTUNG folgendermaßen aktiviert:

Datenträgerkontingente aktivieren!

1. *Öffnen Sie die* COMPUTERVERWALTUNG *unter* START-PROGRAMME-VERWALTUNG-COMPUTERVERWALTUNG.
2. *Klicken Sie auf das Verzeichnis* DATENTRÄGERVERWALTUNG.
3. *Zeigen Sie in der Datenträgerverwaltung mit dem Mauszeiger auf das Laufwerk, für das Kontingente eingerichtet werden sollen.*
4. *Drücken Sie auf die rechte Maustaste und klicken Sie auf* EIGENSCHAFTEN.
5. *Klicken Sie die Registerkarte* KONTINGENT *an und aktivieren Sie die* KONTINGENTVERWALTUNG.
6. *Beschränken Sie für das Laufwerk den Speicherplatz auf eine den Arbeitsverhältnissen der Benutzer angemessene Kapazität.*
7. *Legen Sie fest, ob die Speicherung nach Erreichen der Kapazitätsgrenze vom System verweigert werden soll.*
8. *Legen Sie ggf. fest, ob eine Warnmeldung ausgegeben werden soll (Statusanzeige für den Administrator), wenn die Warnstufe und/oder die Kapazitätsgrenze erreicht wird.*

Über die Schaltfläche KONTINGENTEINTRÄGE wird in einem weiteren Fenster der Status der Kontingentverwaltung angezeigt. Darüber hinaus können Kontingente benutzerspezifisch angepasst, deaktiviert oder gelöscht werden. Es gelten dann nicht mehr die allgemeinen vorgegebenen Kapazitätsgrenzen.

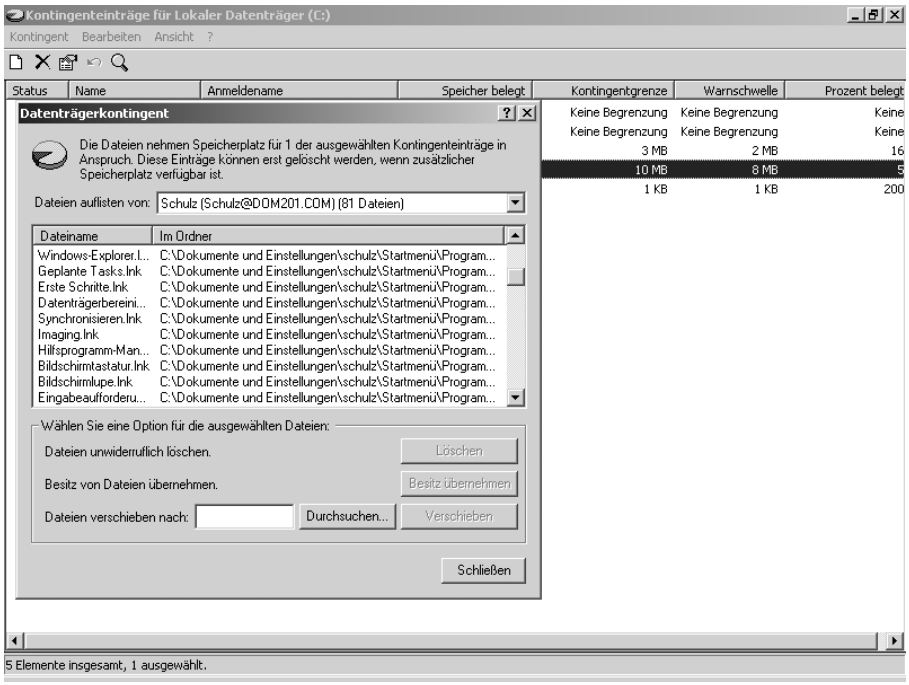


Datenträgerkontingent benutzerspezifisch einrichten

- Die Kontingentverwaltung lässt sich nur auf Laufwerken einsetzen, die unter Windows 2000 mit NTFS formatiert wurden.
- Die in der Registerkarte durchgeführten Einstellungen gelten zunächst automatisch für alle Benutzer, die auf dem entsprechenden Laufwerk Daten speichern.
- Datenträgerkontingente berücksichtigen keine Komprimierung von NTFS-Laufwerken. Alle Dateien werden in ihrer vollen Größe auf die Kontingente angerechnet, ohne Rücksicht auf die tatsächliche Speicherplatzgröße, die sie auf einem komprimierten NTFS-Laufwerk belegen.

Nur über das Menü KONTINGENT-KONTINGENTEINTRAG LÖSCHEN kann das für einen Benutzer erstellte Kontingent eingesehen werden. Nach Auswahl werden alle dem Benutzer zugeordneten Dateien angezeigt. Der Administrator kann Dateien aus dem Kontingent eines Benutzers entfernen, indem er sie durch Markieren löscht, verschiebt oder den Besitz übernimmt.

Die Löschung von Dateien aus dem Kontingent eines Benutzers kann nicht rückgängig gemacht werden. Die Dateien werden nicht in den Papierkorb verlagert, sondern von dem Laufwerk **unwiederbringlich** entfernt.



Datenträgerkontingent löschen

- Wird auf dem Stammlaufwerk (C:\) der Clients die Kontingentverwaltung aktiviert, werden auch die Ordner des Benutzerprofils (Desktop) in das Kontingent des Benutzers mit einbezogen. Dateien, die in den Papierkorb verschoben werden, belasten das Kontingent ebenfalls so lange, bis der Papierkorb geleert wird.

- Durch die Besitzübernahme wird der Administrator Besitzer der Datei. Die Datei wird aus dem Kontingent des Benutzers entfernt. Die Zugriffsrechte bleiben unverändert.

- Ein Verschieben von Dateien ist nur auf einen anderen Datenträger möglich. Dabei geht der Besitz an den Dateien auf den Administrator über. Die Zugriffsrechte der Dateien erben die Rechte des Ordners, in den sie verschoben werden.

Folgendes ist bei der Aktivierung der Kontingentverwaltung zu berücksichtigen:

- *Die Aktivierung der Kontingentverwaltung sollte sorgfältig geplant werden.*

- *Die Aktivitäten der Benutzer auf den Systemen können mittels der Kontingentverwaltung umfassend **sicherheitstechnisch** kontrolliert werden. Beispielsweise können nicht erlaubte Softwareinstallationen oder die Nichtbeachtung von Löschungsfristen laufwerksbezogen ermittelt werden.*

- *Es ist festzulegen, welche Server- und Clientlaufwerke mit der Kontingentverwaltung einzurichten sind. Grundsätzlich sollten die Laufwerke in die Kontingentverwaltung einbezogen werden, auf denen ein Benutzer Zugriffsrechte erhält.*

- *Auf dem Server und dem Client muss ebenfalls definiert werden, wie viel Speicherplatzkapazität den Benutzern jeweils zur Verfügung gestellt wird.*

- *Des Weiteren ist festzulegen, welche Person in welchen Zeitabständen die Verwaltung bzw. Überprüfung durchführt und wie zu reagieren ist, wenn Verstöße gegen die Sicherheitsvorgaben festgestellt werden.*

8.8 Sicherheitscheck

- *Setzen Sie ein Tool ein, mit dem Sie die Freigabe- und NTFS-Berechtigungen nachvollziehbar ordnerbezogen und/oder benutzerbezogen **transparent** machen können (siehe Kapitel 11).*

- *Planen Sie, welche **Ressourcen** freigegeben werden müssen. Berücksichtigen Sie dabei, dass bereits eine Reihe administrativer verdeckter Freigaben erstellt sind.*

- *Geben Sie nur die Ressourcen frei, auf die die Benutzer über das **Netzwerk** zugreifen müssen.*

- *Weisen Sie die **Freigabeberechtigungen** Gruppen- und nicht Benutzerkonten zu, um die Zugriffsverwaltung einfacher zu gestalten.*

- *Berücksichtigen Sie, dass mit der Erstellung einer Freigabe grundsätzlich immer die Gruppe **JEDER** mit **VOLLZUGRIFF** zugewiesen wird. Entfernen Sie die Gruppe ggf. und vergeben Sie nur so viele Rechte wie nötig.*

- *Beachten Sie, dass die dem Benutzer zugeordneten freigegebenen Ressourcen in die **Desktop-Oberfläche** integriert werden. Der Benutzer sollte keinen Zugriff auf die Netzwerkumgebung erhalten (siehe Kapitel 10).*

- *Vergeben Sie NTFS-Berechtigungen auf Ordner- und Dateiebene.*

- *Um die NTFS-Berechtigungsvergabe nachvollziehbar zu gestalten, verwenden Sie nach Möglichkeit die vorgegebenen **Schablonen**. Vergeben Sie nur Detailrechte, wenn spezielle Anforderungen vorliegen.*

- *Geben Sie den Benutzer- und Gruppenkonten keine **Vollzugriffsrechte** auf Ordner und Dateien. Weisen Sie das Mindestmaß an erforderlichen Berechtigungen zu.*

- *Beachten Sie, dass Benutzer nicht die Berechtigungen erhalten, vorgegebene **Ordnerstrukturen** (z. B. die zentrale Datenablage) zu verändern.*

- *Überprüfen Sie die **ordnungsgemäße** Berechtigungsvergabe, indem Sie sich unter dem entsprechenden Benutzerkonto anmelden, dem Sie Berechtigungen zugewiesen haben.*

- *Beachten Sie, dass bei der **Kombination** von Freigabe- und NTFS-Berechtigungen die Berechtigung mit der größten Einschränkung berücksichtigt wird.*

- ***Verweigern** Sie einem Benutzer- bzw. Gruppenkonto nur dann NTFS-Berechtigungen, wenn es über ein anderes Gruppenkonto nicht erwünschte Berechtigungen erhalten hat.*

- *Berücksichtigen Sie, dass der **Ersteller** eines Ordners Vollzugriff auf diesen erhält. Er kann somit die NTFS-Berechtigungen administrieren. In einer zentralen Datenablage könnte so der Zugriff der Administration entzogen werden. Nur über die **Besitzübernahme** könnte sich die Administration Zugriff verschaffen. Dies hinterlässt jedoch „Spuren", da der Besitzer ohne den Einsatz von „Hacker-Tools" nicht übertragbar ist.*

- *Setzen Sie die **Verschlüsselung** (EFS) auf mobilen PC ein, damit die Daten bei Diebstahl des Systems geschützt sind.*

- *Bedenken Sie, dass auf internen Systemen die Datenabschottung bereits über Freigabe- und NTFS-Berechtigungen realisiert werden kann. Der Einsatz der Verschlüsselung macht hier nur dann Sinn, wenn der Zugriff der **administrativen Ebene** verhindert werden soll.*

- *Das Administratorkonto verfügt standardmäßig über die Funktion des **Datenwiederherstellungsagenten**. Diesem ist diese Funktion bei Einsatz der Verschlüsselung von Ordnern und Dateien zu entziehen.*

- *Berücksichtigen Sie, dass Benutzer auf vielen standardmäßig eingerichteten Ordnern die Verschlüsselung aktivieren können. **Entziehen** Sie diesen Ordnern ggf. die NTFS-Berechtigung ATTRIBUTE SCHREIBEN.*

- *Aktivieren Sie die **Datenträgerkontingentverwaltung** auf den Servern und Clients. Es sind Zuständigkeiten für die **Überwachung** der Kontingentverwaltung festzulegen.*

9 Lokale Sicherheitsrichtlinien

In diesem Kapitel erfahren Sie,

- den Unterschied zwischen *Lokalen* und *Active Directory-Sicherheitsrichtlinien*,
- wie die Kennwort- und Kontosperrungsrichtlinien eingestellt werden sollten,
- wie mithilfe der Benutzer- bzw. Systemrechte die Befugnisse der Administratoren eingeschränkt werden können und
- welche Bedeutung die Sicherheitsoptionen haben.

9.1 Überblick und Einsatz

9.1.1 Lokale und Active Directory-Sicherheitsrichtlinien

Im Vergleich zu Windows NT sind unter Windows 2000 die Richtlinien erheblich erweitert und umstrukturiert worden.

Unter Windows NT werden die Richtlinien mit verschiedenen Programmen umgesetzt. So werden z. B. mit dem Benutzermanager die Benutzerrechte sowie die Konto- und Überwachungsrichtlinien administriert, während mithilfe des **Systemrichtlinien-Editors** weiter gehende Richtlinien computer- und benutzerbezogen festgelegt werden können, die die Funktionen des Clients/Benutzers einschränken.

Unter Windows 2000 sind diese Richtlinien nun zu so genannten **Gruppenrichtlinien** zusammengefasst worden. Es werden *Lokale Sicherheitsrichtlinien* und *Active Directory-Sicherheitsrichtlinien* unterstützt.

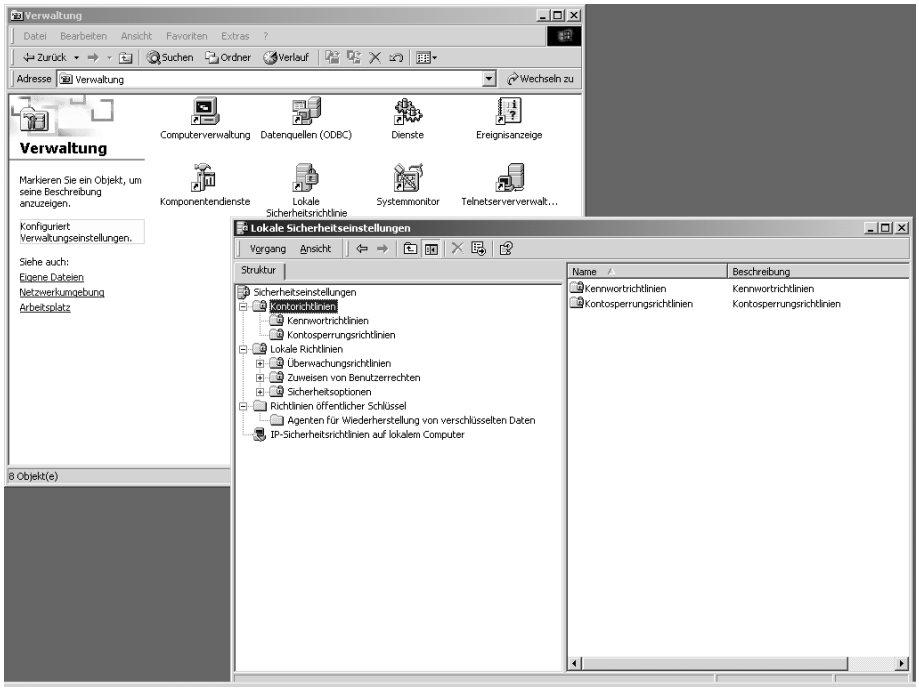
Die *Active Directory-Sicherheitsrichtlinien* unterscheiden sich von den *Lokalen Sicherheitsrichtlinien* in der Wirkungsweise. Der Umfang und die Strukturen der Richtlinien sind nahezu identisch. In Kapitel 10 wird der Einsatz der *Active Directory-Richtlinien* in einer Domänenumgebung beschrieben, während in diesem Kapitel zunächst die Sicherheitseinstellungen der *Lokalen Sicherheitsrichtlinien* (siehe Abbildung) erläutert werden. Diese Richtlinien haben eine grundsätzliche Bedeutung, da sie auch auf Einzelplatz-PC bzw. in einer Arbeitsgruppe aktiviert werden sollten.

9.1.2 Lokale Sicherheitseinstellungen/Richtlinien

Die *Lokalen Sicherheitsrichtlinien* befinden sich auf jedem Windows 2000-Computer. Sie wirken sich auf die Funktionen des **Computers** und auf **alle Benutzer** aus, die sich an diesem Computer anmelden. Eine differenzierte benutzerbezogene Richtlinienzuordnung ist mit Ausnahme der Richtlinien *Zuweisen von Benutzerrechten* nicht möglich.

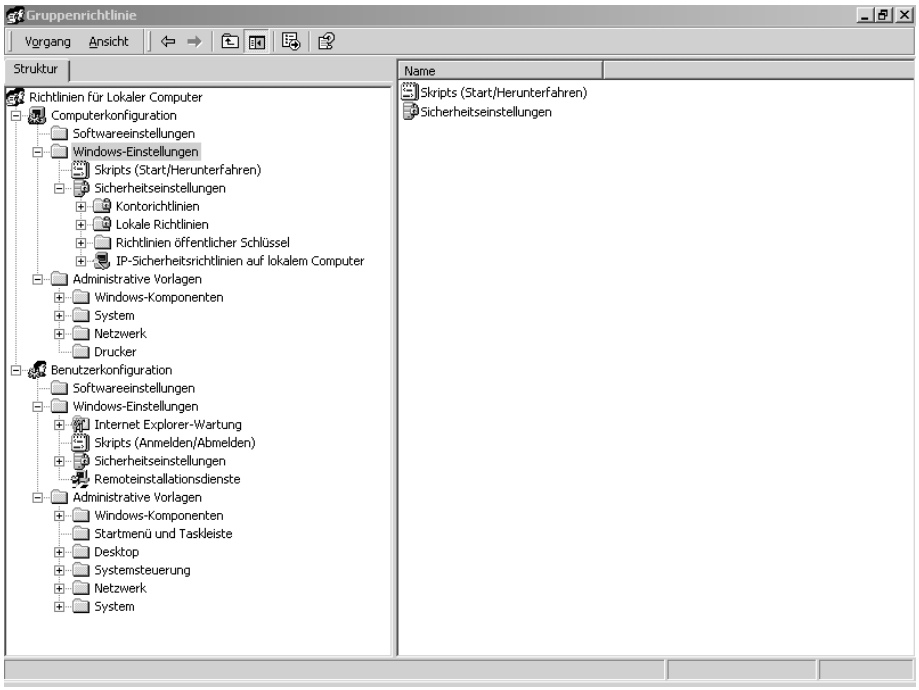
Beachten Sie, dass sich die meisten *Lokalen Richtlinien* auch auf die Administratorkonten auswirken. Sie sollten deshalb die Konfiguration der *Lokalen Richtlinien* sehr überlegt durchführen. Deaktivieren Sie z. B. zu viele Funktionen, kann es passieren, dass Sie unter einem Administratorkonto diese Einstellungen nicht mehr rückgängig machen können, weil Sie selbst nicht mehr über die Berechtigung verfügen.

Aufgrund der umfangreichen Einstellungsmöglichkeiten und damit verbundenen Möglichkeiten, die Funktionen des Systems einzuschränken, stellt Microsoft die Richtlinien in unterschiedlichen Verwaltungsprogrammen zur Verfügung. Das auf dem Desktop unter dem Ordner VERWALTUNG integrierte Programm *Lokale Sicherheitseinstellungen* enthält nur einen **Ausschnitt** der *Lokalen Sicherheitsrichtlinien*.



Lokale Sicherheitseinstellungen Windows 2000 Professional

Die **vollständigen** *Lokalen Richtlinien* können unter START-AUSFÜHREN mit dem Verwaltungsprogramm *gpedit.msc* aufgerufen werden. Sie enthalten den „Knoten“ SICHERHEITSEINSTELLUNGEN (siehe Abbildung) und werden auf dem lokalen Datenträger in dem Ordner <Stammverzeichnis:\Winnt\System32\GroupPolicy> gespeichert.



Richtlinien für Lokale Computer

Die *Lokalen Sicherheitsrichtlinien* haben insbesondere dann eine Bedeutung, wenn die Computer **nicht** in einer Domäne integriert sind.

Folgendes ist beim Einsatz von Sicherheitsrichtlinien zu berücksichtigen:

- *Windows 2000 aktiviert mit der Installation standardmäßig Richtlinien im Bereich der BENUTZERRECHTE und der SICHERHEITSOPTIONEN.*
- *Planen und dokumentieren Sie, welche Richtlinien in welcher Systemumgebung umgesetzt werden sollen.*
- *Wird der Computer in einer Domäne eingesetzt, ist die Administration der LOKALEN SICHERHEITSRICHTLINIEN nur begrenzt erforderlich.*

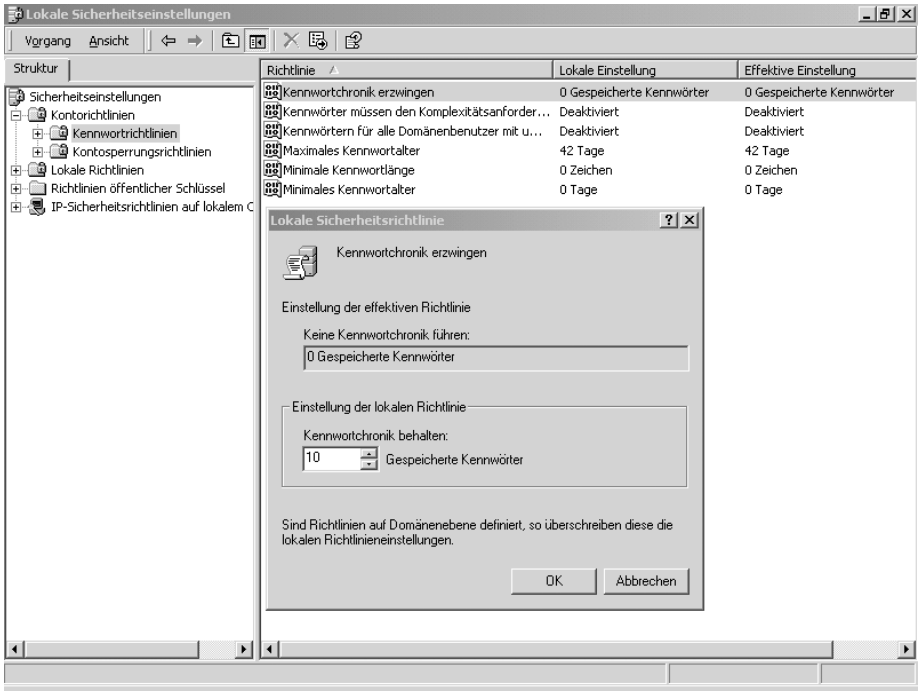
9.2 Lokale Sicherheitsrichtlinien administrieren

Die *Lokalen Sicherheitsrichtlinien* befinden sich auf **jedem** Windows 2000-System unter der Systemsteuerung im Ordner VERWALTUNG. Die Konfiguration der Sicherheitsrichtlinien ist durch die Auswahl der entsprechenden Richtlinie und nach Eintragung des gewünschten Parameters bzw. durch das Aktivieren oder Deaktivieren einfach durchzuführen. Danach werden im rechten Fenster die durchgeführten Einstellungen in der Spalte LOKALE EINSTELLUNG angezeigt. In der Spalte EFFEKTIVE EINSTELLUNG werden hingegen immer die vom System umgesetzten Richtlinien dargestellt. Diese Spalte hat nur dann eine Bedeutung, wenn die Computer in eine **Domäne** integriert werden und neben den *Lokalen Richtlinien* zusätzlich *Active Directory-Richtlinien* umsetzen.

Einige *Lokale Richtlinien* werden erst nach einer **erneuten** Benutzeranmeldung aktiv. Dazu zählen vor allem die Richtlinien unter ZUWEISEN VON BENUTZERRECHTEN. Andere Richtlinien erfordern sogar den Neustart des Computers.

9.3 Kontorichtlinien

9.3.1 Kennwortrichtlinien



Kennwortrichtlinie Kennwortchronik erzwingen

Kennwortchronik erzwingen
Empfohlene Einstellung: 10
Benutzte Kennwörter werden aufbewahrt, sodass der Benutzer systemseitig gezwungen wird, ein neues Kennwort zu wählen. Er kann ein altes Kennwort erst dann wieder verwenden, wenn es nicht mehr in der Kennwortchronik geführt wird. Bei 10 gespeicherten Kennwörtern könnte der Benutzer erst beim 11. Kennwortwechsel das erste gewählte Kennwort wieder verwenden.

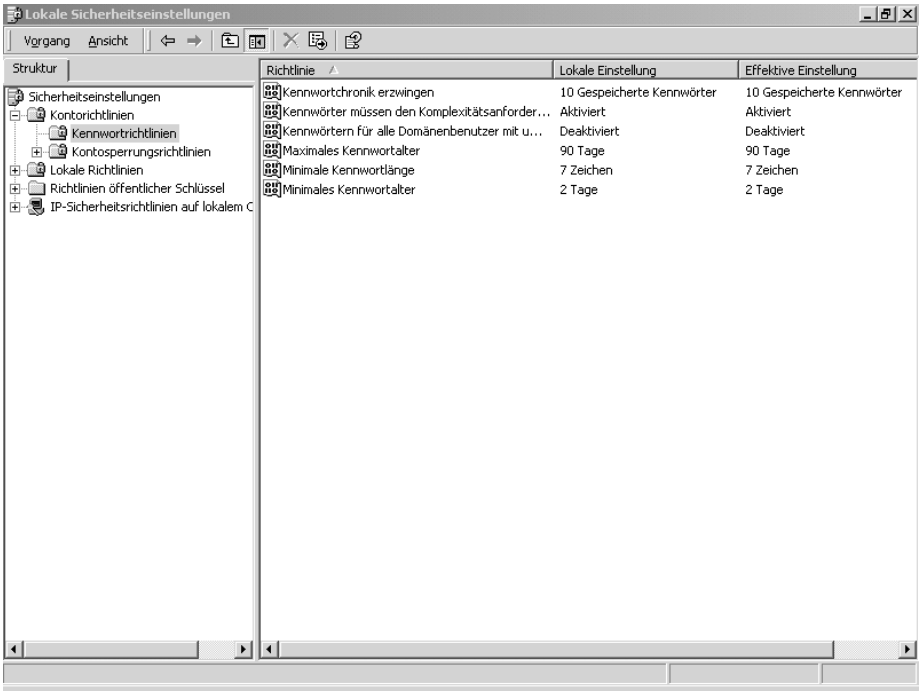
Kennwortchronik der Lokalen Sicherheitsrichtlinien aktivieren!

1. *Rufen Sie unter START-PROGRAMME-VERWALTUNG bzw. START-SYSTEMSTEUERUNG-VERWALTUNG die LOKALE SICHERHEITSRICHTLINIE auf.*
2. *Klicken Sie mit der linken Maustaste auf KONTORICHTLINIEN und danach auf KENNWORTRICHTLINIEN.*
3. *Im rechten Fenster doppelklicken Sie mit der linken Maustaste auf die Richtlinien KENNWORTCHRONIK ERZWINGEN.*
4. *Geben Sie im neu geöffneten Eigenschaftenfenster die Anzahl der zu speichernden Kennwörter ein und bestätigen Sie mit OK. Die Richtlinie wird sofort aktiv, ohne dass eine erneute Anmeldung notwendig ist.*

Kennwörter müssen den Komplexitätsanforderungen entsprechen
Empfohlene Einstellung: Aktiviert
Nach Aktivierung dieser Richtlinie muss der Benutzer ein Kennwort verwenden, • das den Benutzernamen oder Teile davon nicht enthalten darf, • das Zeichen aus mindestens drei der Kategorien Großbuchstaben, Kleinbuchstaben, Ziffern und Satz- bzw. Sonderzeichen enthält, • das den Richtlinien MINIMALE KENNWORTLÄNGE und KENNWORTCHRONIK unterliegt.

Kennwörter für alle Domänenbenutzer mit umkehrbarer Verschlüsselung speichern
Empfohlene Einstellung: Deaktiviert
Der Austausch von verschlüsselten Kennwörtern zwischen einem Domänencontroller und einem Client mit „fremden“ Betriebssystemen (Unix, Macintosh) kann zu Problemen führen. Einige ältere „Nicht-Microsoft“-Betriebssysteme sind zu den Windows 2000-Anmeldemechanismen nicht kompatibel. Durch die Aktivierung dieser Option wird ein zweites einfach verschlüsseltes Kennwort – ein so genantes LANMAN-Kennwort – gespeichert, sodass die Kompatibilität zu älteren Betriebssystemen gewährleistet ist.

Maximales Kennwortalter
Empfohlene Einstellung: max. 90
Gibt an, wie viele Tage ein Kennwort gültig ist. Der Benutzer wird vor Ablauf des Kennwortes aufgefordert, sein Kennwort zu wechseln.



Aktivierte Kennwortrichtlinien

Minimale Kennwortlänge
Empfohlene Einstellung: 7
Das Kennwort kann eine Länge zwischen 0 und 14 Zeichen haben. Die Einstellung 0 bedeutet, dass das Benutzerkonto über kein Kennwort verfügt. Zu lange Kennwörter sind nicht sehr benutzerfreundlich. Es besteht dann die Gefahr, dass Kennwörter am Arbeitsplatz hinterlegt werden. Eine Kennwortlänge von 7 Zeichen ist hinreichend sicher und für den Benutzer praktikabel.

Minimales Kennwortalter
Empfohlene Einstellung: 2
Das minimale Kennwortalter gibt die Zeit in Tagen vor, an denen systemseitig keine Kennwortänderung durch den Benutzer erlaubt wird. Diese Einstellung ist dann von Bedeutung, wenn die Kennwortchronik aktiviert wurde. Ein Benutzer könnte ansonsten den dauerhaften Wechsel zu einem neuen Kennwort umgehen, indem er so lange neue Kennwörter eingibt, bis er zu seinem alten Kennwort zurückkehrt. Ist jedoch die Richtlinie MINIMALES KENNWORTALTER aktiviert, wird die Rückkehr zu dem alten Kennwort erheblich erschwert.

Beachten Sie, dass die Kennwörter der Domänenbenutzerkonten in der Active Directory-Datenbank des Domänencontrollers und die Kennwörter der lokalen Benutzerkonten in der SAM-Datenbank der Clients trotz Verschlüsselung von Windows 2000 nicht hinreichend sicher verwaltet werden.

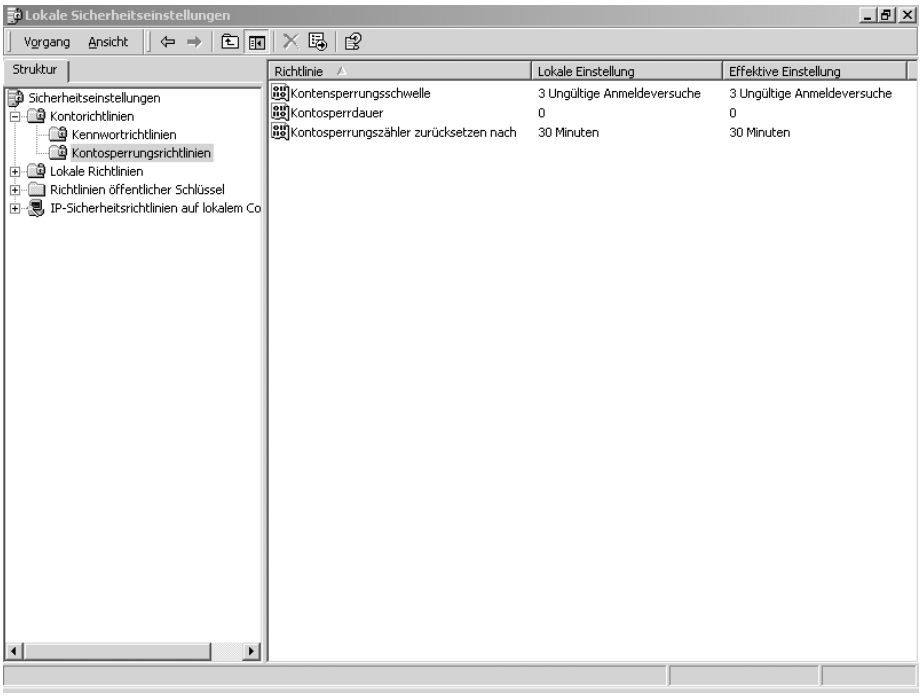
Mithilfe einer **Passwortcrack-Software** (siehe Kapitel 13, www.atstake.com, L0phtcrack) können die Kennwörter entschlüsselt werden, sofern ein Benutzer über den Zugriff auf die entsprechenden Dateien verfügt. Sie werden in den folgenden Ordnern gespeichert:

Active Directory-Datenbank (Standardpfad):	\Winnt\NTDS\ntds.dit
SAM-Datenbank (Clients- und Mitgliedserver):	\Winnt\system32\config\sam
Sicherungsordner der SAM-Datenbank:	\Winnt\repair\sam

Die Einstellungen unter den **Kontooptionen** der einzelnen Benutzerkonten im Verwaltungsprogramm *Active Directory-Benutzer und -Computer* werden **vorrangig** umgesetzt. Wird z. B. bei einem Benutzerkonto die Kontooption KENNWORT LÄUFT NIE AB aktiviert und gleichzeitig die Kennwortrichtlinie MAXIMALES KENNWORTALTER auf 90 Tage gesetzt, dann erhält der Benutzer keine systemseitige Aufforderung, sein Kennwort zu ändern.

9.3.2 Kontosperrungsrichtlinien

Kontosperrungsschwelle
Empfohlene Einstellung: 3
Die Kontosperrungsschwelle legt fest, wie oft ein Benutzer das Kennwort falsch eingeben kann, bevor sein Benutzerkonto gesperrt wird. Wird diese Richtlinie aktiviert, werden die Werte der Richtlinien KONTOSPERRDAUER und KONTOSPERRUNGSZÄHLER ZURÜCKSETZEN NACH standardmäßig auf jeweils 30 Minuten geändert und müssen ggf. angepasst werden.



Aktivierte Kontosperrungsrichtlinien

Kontosperrdauer
Empfohlene Einstellung: 0
Über die Kontosperrdauer wird bestimmt, wie viele Minuten das Konto gesperrt bleibt. Die Einstellung 0 bewirkt, dass das Benutzerkonto deaktiviert wird und nur durch den Administrator entsperrt werden kann (für mobile PC nicht unbedingt sinnvoll). Das hat den Vorteil, dass der Administrator den Benutzer befragen kann, ob er die Sperrung selbst verursacht hat. Ist die Kontosperrung nicht auf ihn zurückzuführen, sind möglicherweise unter seinem Benutzerkonto unberechtigte Anmeldeversuche durch einen „fremden“ Benutzer durchgeführt worden. Die Administration ist somit gewarnt, dass ein Benutzer versucht, das System unberechtigt zu nutzen.

Kontosperrungszähler zurücksetzen nach
Empfohlene Einstellung: 30
Fehlerhafte Anmeldeversuche werden nach Ablauf einer vorgegebenen Zeit wieder auf 0 gesetzt. Meldet sich z. B. ein Benutzer nach zwei fehlerhaften Anmeldeversuchen erfolgreich am System an, steht der Kontosperrungszähler auf 2. Ist die Kontosperrungsschwelle auf 3 eingestellt, hätte der Benutzer noch einen fehlerhaften Anmeldeversuch, bevor sein Konto gesperrt wird. Ist für das Zurücksetzen des Kontosperrungszählers z. B. eine Zeit von 30 Minuten eingestellt, verfügt der Benutzer nach Ablauf dieser Frist wieder über 3 neue Anmeldeversuche.

9.4 Lokale Richtlinien

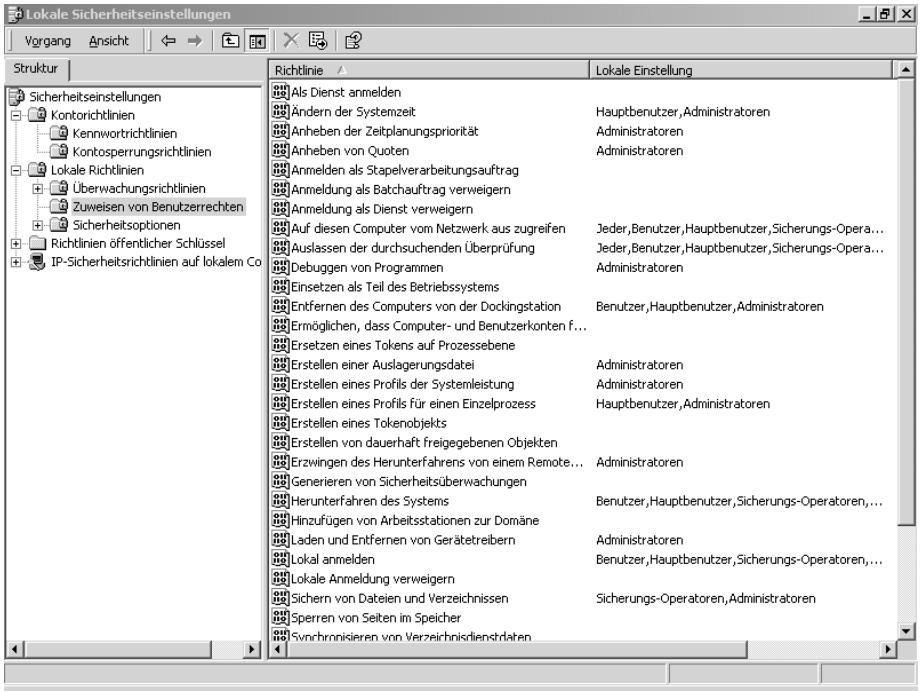
9.4.1 Überwachungsrichtlinien

Der Einsatz der lokalen Überwachungsrichtlinien sollte davon abhängig gemacht werden, in welcher (System-)Umgebung der Computer eingesetzt wird. Die Aktivierung auf Einzelplatz-PC ist in der Regel nur mit einem **minimalen Sicherheitsgewinn** verbunden. Deshalb sollte auf einem Einzelplatz-PC ggf. nur die Überwachungsrichtlinie ANMELDEVERSUCHE ÜBERWACHEN aktiviert werden. Ihr Einsatz ist hingegen in einer Domänenumgebung sehr viel bedeutsamer. Die Überwachungsrichtlinien werden deshalb in Kapitel 10 gesondert beschrieben.

9.4.2 Zuweisen von Benutzerrechten (Systemrechte)

Unter der lokalen Richtlinie ZUWEISEN VON BENUTZERRECHTEN befinden sich ca. 34 systemspezifische Privilegien, die teilweise einigen Benutzer- und Gruppenkonten zugewiesen sind. Die Benutzerrechte beziehen sich überwiegend auf administrative Aufgaben, wie z. B. das ERSTELLEN EINER AUSLAGERUNGSDATEI, das HINZUFÜGEN VON ARBEITSSTATIONEN ZUR DOMÄNE oder das SICHERN VON DATEIEN UND VERZEICHNISSEN. Nur wenige Benutzerrechte sind für den Benutzer bzw. Anwender von Bedeutung. Hierzu zählen z. B. das HERUNTERFAHREN DES SYSTEMS, die LOKALE ANMELDUNG (auf einem Client) oder ggf. das ÄNDERN DER SYSTEMZEIT.

Über die Benutzerrechte können die **Befugnisse der Administratoren** erheblich eingeschränkt werden. Das ist insbesondere dann von Bedeutung, wenn mehrere Administratoren in einer Organisation tätig sind. So könnten z. B. die Befugnisse für das SICHERN VON DATEIEN UND VERZEICHNISSEN (Datensicherung) die VERWALTUNG DES SICHERHEITSPROTOKOLLS in der Ereignisanzeige oder das ÜBERNEHMEN DES BESITZES VON DATEIEN UND OBJEKTEN bestimmten Administratorkonten zugeordnet werden, die jedoch dann Mitglied in einer der vordefinierten Administratorengruppen (z. B. Kontenoperatoren) werden müssten. Es kann einem Administratorkonto auch das Recht entzogen werden, über das Netzwerk auf einen Computer zuzugreifen.



Zuweisen von Benutzerrechten (Systemrechte)

Beachten Sie, dass unter den LOKALEN SICHERHEITSEINSTELLUNGEN auf jedem Computer von Windows 2000 **standardmäßig** Benutzerrechte vergeben werden. Der Gruppe ADMINISTRATOREN sind die meisten Befugnisse zugewiesen worden. Sofern Sie mehrere administrative Benutzerkonten angelegt haben, erhalten diese automatisch die gleichen Rechte, weil sie Mitglied der Gruppe ADMINISTRATOREN werden.

Nachfolgend werden einige für die Administration wichtige Benutzerrechte erläutert. Der in Klammern befindliche Name stammt aus der englischen Version. Dieser wird z. B. im Sicherheitsprotokoll in der Ereignisanzeige (siehe Tz. 10.6.4) verwendet.

- **Auf diesem Computer vom Netzwerk aus zugreifen (SeNetworkLogonRight)**

  Die zugewiesenen Benutzer- und Gruppenkonten erhalten das Recht, von einem Computer über das Netzwerk auf die Ressourcen dieses Computers, wie z. B. freigegebene Ordner, Drucker, CD-ROM- oder Festplattenlaufwerke, zuzugreifen.

- **Hinzufügen von Arbeitsstationen zu einer Domäne (SeMachineAccountPrivilege)**

  Eine Arbeitsstation muss Mitglied einer Domäne sein, damit sich ein Benutzer an der Domäne anmelden kann. Wird dieses Recht einem Benutzer- oder Gruppenkonto zugewiesen, können unter diesem Konto Arbeitsstationen in die Domäne integriert werden.

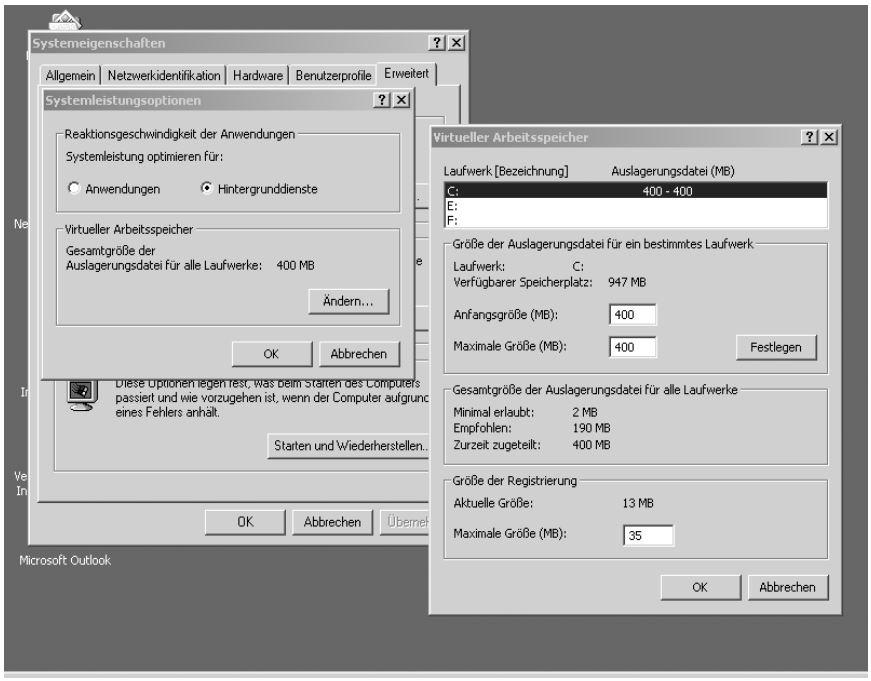
- **Sichern von Dateien und Verzeichnissen (SeBackupPrivilege), Wiederherstellen von Dateien und Verzeichnissen (SeRestorePrivilege)**

  Diese Rechte erlauben einem Benutzerkonto die Datensicherung (Backup) und Datenrücksicherung (Restore) durchzuführen. Diese administrativen Aufgaben können einem gesonderten Benutzerkonto zugewiesen werden, das nicht gleichzeitig auch der Gruppe *Administratoren* zugeordnet wurde. Eine Abgrenzung der administrativen Zugriffe auf das System ist somit gewährleistet.

- **Erstellen einer Auslagerungsdatei (SeCreatePageFilePrivilege)**

  Dieses Systemrecht wird benötigt, wenn z. B. eine neue Auslagerungsdatei eingerichtet werden muss. Windows 2000 erstellt bereits mit der Installation eine Auslagerungsdatei für die kurzfristige **Zwischenspeicherung** der im Hauptspeicher verarbeiteten Daten. Die Auslagerungsdatei erhält keine konstant vorgegebene Größe, sondern einen Kapazitätsbereich, der je nach Festplattengröße ca. zwischen 150 MB und 400 MB liegen kann. Die Datei wächst also mit zunehmender Nutzung des Systems. Dadurch wird die Datei jedoch

auf der Festplatte zerstückelt (fragmentiert) verwaltet, was zur Verringerung der Performance des Systems beiträgt. Das in Windows 2000 enthaltene Defragmentierungsprogramm defragmentiert die Auslagerungsdatei nicht. Es sollte deshalb die Anfangsgröße und der Maximalwert gleichgesetzt werden. Damit ist sichergestellt, dass die Datei eine konstante Größe beibehält. Des Weiteren sollte ein Defragmentierungstool (siehe Kapitel 11, www.sysinternals.com, pagedfrg) installiert werden, das u. a. die **Systemdateien** (Pagefile.sys, SAM, Registrydateien) nach jeder Bootphase defragmentiert.



Virtueller Arbeitsspeicher (Auslagerungsdatei)

- **Ändern der Systemzeit (SeSystemtimePrivilege)**

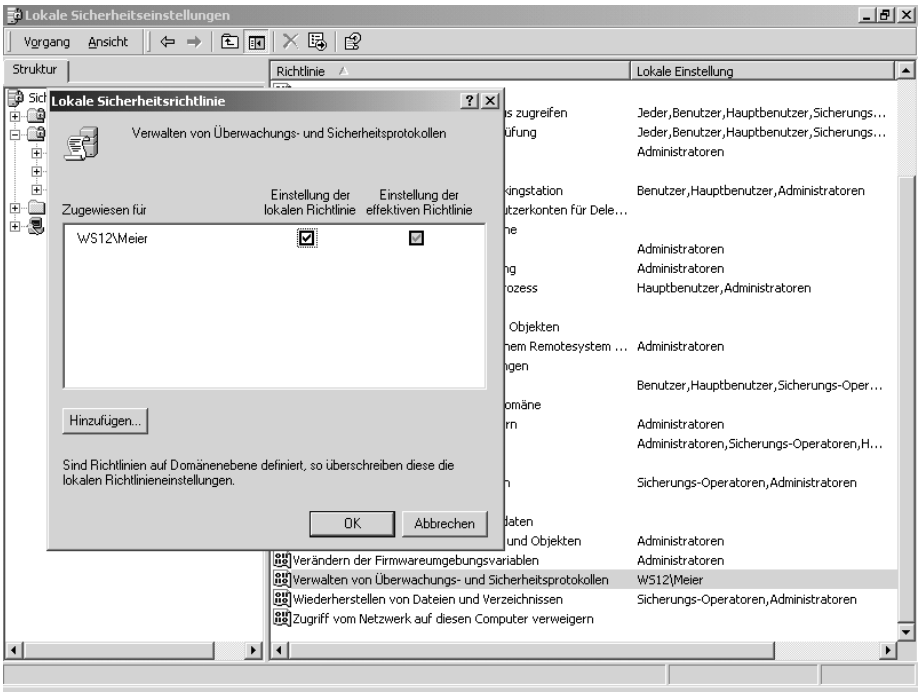
  Die Befugnis zum Ändern der Systemzeit auf dem Computer ist nur den Gruppen *Administratoren* und den *Hauptbenutzern* zugewiesen. Weitere Benutzerkonten müssen entsprechend hinzugefügt werden. Wird ein Computer in die Domäne integriert, kommt es zu einer automatischen **Zeitsynchronisierung** zwischen Client und Domänencontroller, d. h., die Uhrzeit des Domänencontrollers wird auf den Client übertragen.

- **Laden und Entfernen von Geräte-Treibern (SeLoadDriverPrivilege)**

  Das Recht, Gerätetreiber zu administrieren, ist ausschließlich der Gruppe *Administratoren* zugeordnet. Auch für diesen Bereich ist eine Abgrenzung administrativer Aufgaben denkbar. Nur die Administratoren, die für die Installation der Systeme zuständig sind, erhalten dann dieses Recht.

- **Verwalten von Überwachungs- und Sicherheitsprotokollen (SeSecurityPrivilege)**

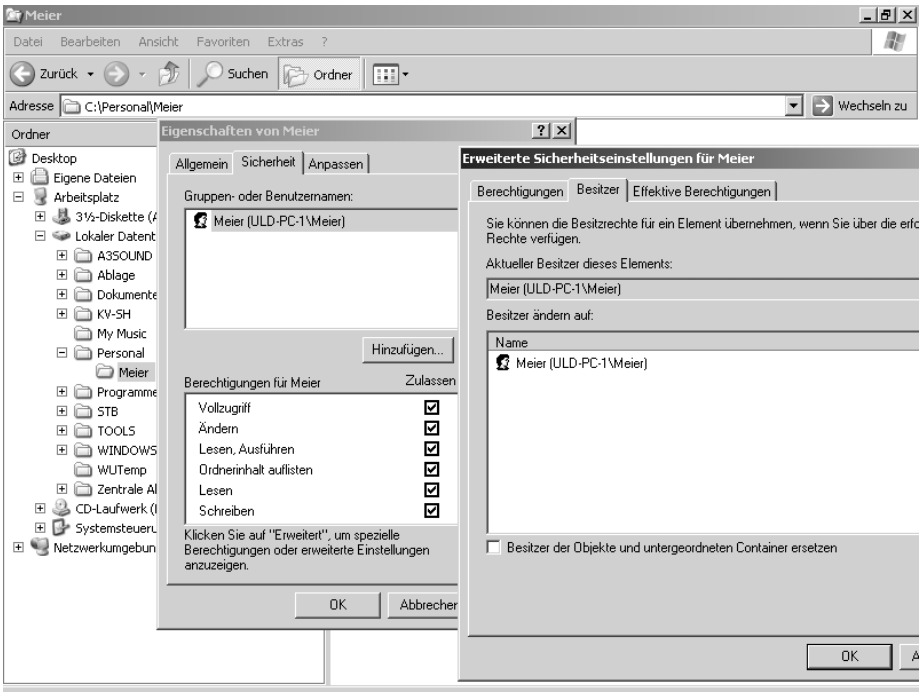
  Das Recht für die Verwaltung des Sicherheitsprotokolls erhält standardmäßig die Gruppe *Administratoren*. Wenn beabsichtigt wird, dass auch administrative Aktivitäten überwacht werden sollen, sollten der Zugriff und die Verwaltung des Sicherheitsprotokolls einer neutralen Abteilung, z. B. dem Datenschutzbeauftragten, zugeordnet werden (siehe Tz. 10.6.4).



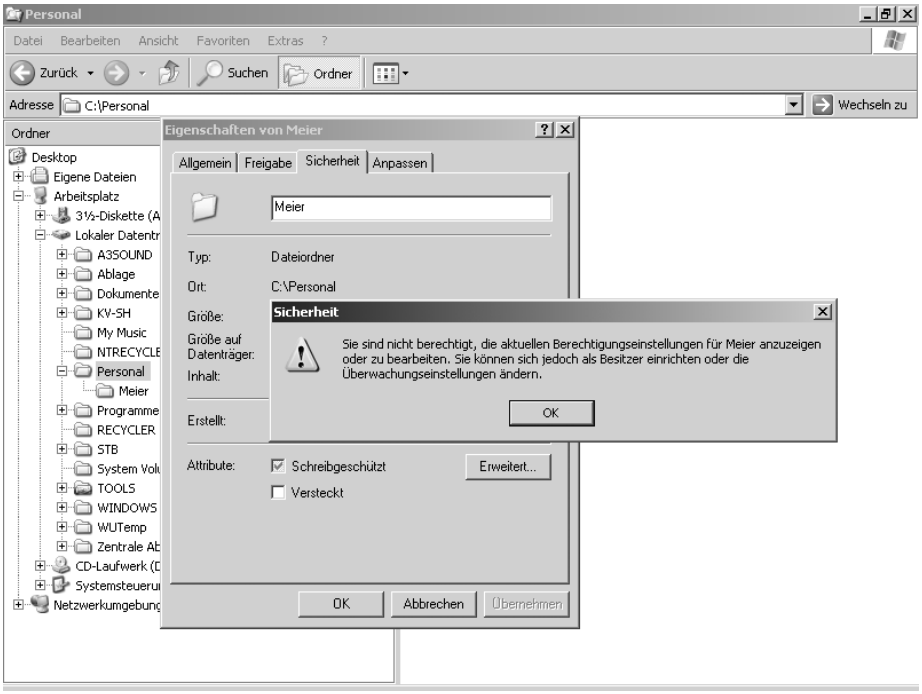
Systemrecht Verwaltung von Überwachungs- und Sicherheitsprotokollen

- **Übernehmen des Besitzes von Dateien und Objekten (SeTakeOwnershipPrivilege)**

  Dieses Recht ist ausschließlich der Gruppe *Administratoren* zugewiesen. Das Übernehmen des Besitzes von Ordnern oder Dateien ist dann von Bedeutung, wenn auf das Objekt aufgrund fehlender NTFS-Berechtigungen nicht zugegriffen werden kann. Das kann z. B. vorkommen, wenn ein Benutzer einen Ordner anlegt und die NTFS-Berechtigungen so weit einschränkt, dass nur noch er selbst auf diesen Ordner zugreifen kann. Da er zudem der BESITZER des Ordners ist, haben auch die Administratoren nicht die Befugnis, die NTFS-Berechtigungen zu verändern. Die Besitzübernahme des Ordners ist die einzige Möglichkeit, auf den Ordner zuzugreifen. Das setzt jedoch voraus, dass das Recht ÜBERNEHMEN DES BESITZES VON DATEIEN UND OBJEKTEN dem entsprechenden Benutzerkonto zugewiesen wurde, das bei allen Benutzerkonten der Gruppe *Administratoren* der Fall ist.



Besitzer des Ordners Meier



Besitzübernahme über das Administratorkonto durchführen

Beachten Sie, dass mit den Standardfunktionen von Windows 2000 der Besitzer eines Ordners nicht übertragen werden kann. Wenn z. B. das Benutzerkonto A Besitzer eines Ordners ist und das Benutzerkonto B den Besitz des Ordners übernimmt, kann B nicht anschließend den Besitz wieder auf A übertragen. Es sind je-

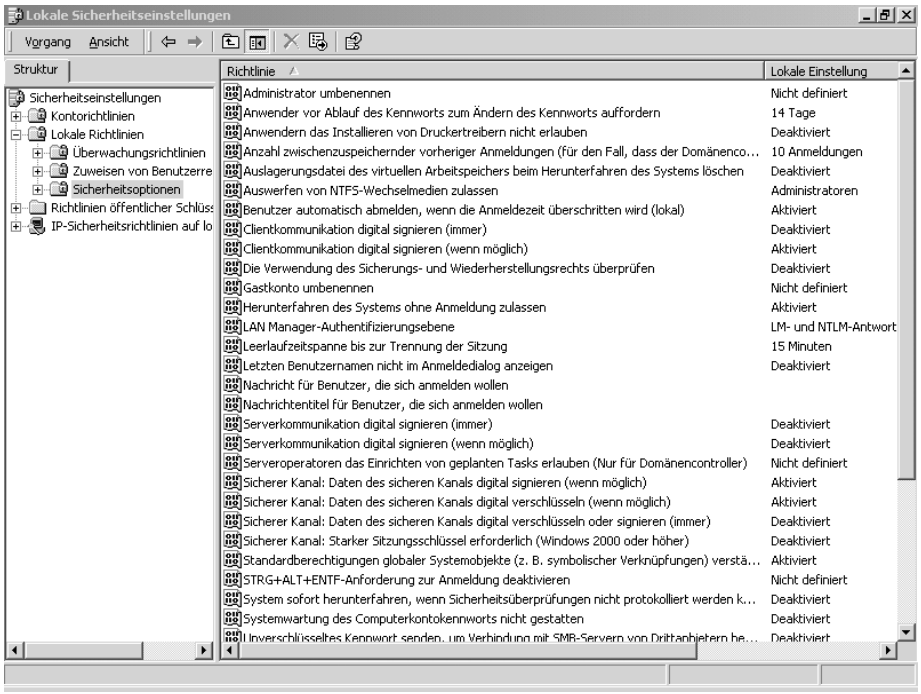
doch im Internet (www.ntsecurity.nu) Tools (z. B. setowner) verfügbar, mit denen der Name eines Benutzerkontos (Besitzer) einem Objekt zugeordnet werden kann.

- **Lokal anmelden (SeInteractiveLogonRight)**

  Nach der Installation von Windows 2000 auf einem Server erhalten nur die administrativen Gruppen die Befugnis zur lokalen Anmeldung, während auf dem Client über die Gruppe *Jeder* alle lokal eingerichteten Benutzerkonten zur Anmeldung zugelassen sind. Sollen weitere Benutzer- oder Gruppenkonten das Recht zur lokalen Anmeldung erhalten, so muss ihnen dieses Recht explizit zugewiesen werden.

9.4.3 Sicherheitsoptionen

Während die Benutzer- bzw. Systemrechte ausschließlich Benutzer- und Gruppenkonten zugewiesen werden können, beziehen sich die **Sicherheitsoptionen** auf einige spezielle **Funktionen** von Windows 2000.



Lokale Richtlinien – Sicherheitsoptionen

Die Sicherheitsoptionen lassen sich entweder aktivieren oder deaktivieren, aber keinem Benutzer- oder Gruppenkonto zuweisen. Nachfolgend werden die wichtigsten Sicherheitsoptionen erläutert:

- **Herunterfahren des Systems ohne Anmeldung zulassen**

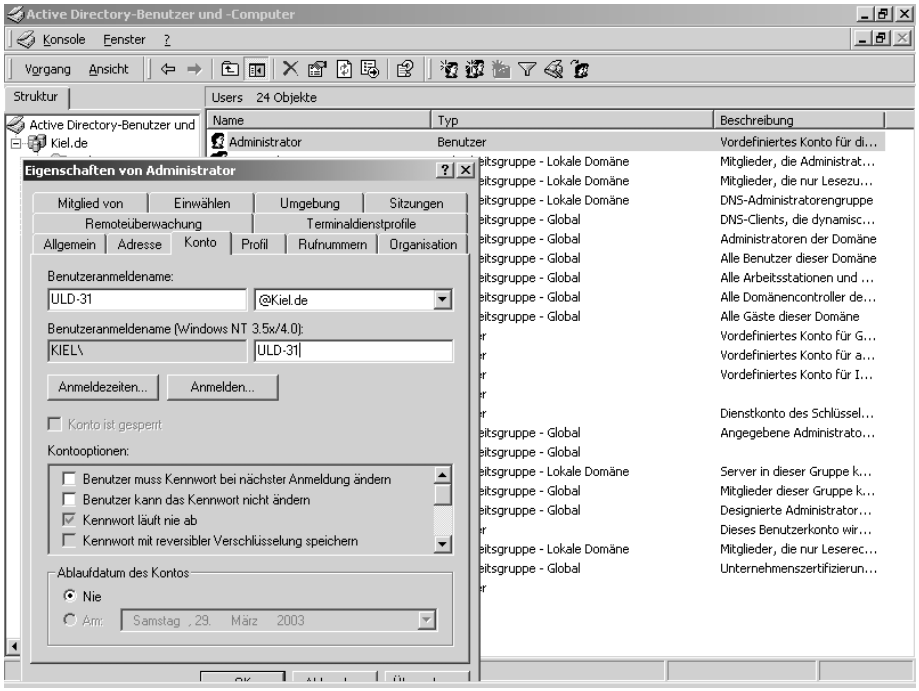
  Über die Schaltfläche HERUNTERFAHREN im Anmeldefenster können Benutzer das System herunterfahren, ohne dass sie sich anmelden müssen. Diese Funktion ist auf **Servern** in den lokalen Richtlinien aus Sicherheitsgründen standardmäßig deaktiviert.

Beachten Sie, dass nach der Installation von Windows 2000 standardmäßig einige Sicherheitsoptionen aktiviert werden. Überprüfen Sie deshalb, welche Sicherheitsoptionen in Bezug auf Ihre Systemumgebung angepasst werden sollten.

- **Administrator umbenennen**

  Mithilfe dieser Sicherheitsoption kann das Administratorkonto (Anmeldename) von Windows 2000 umbenannt werden. Da die Microsoft-Betriebssysteme standardmäßig ein Administratorkonto mit dem Benutzernamen *Administrator* einrichten, bietet es Angriffsmöglichkeiten für Benutzer, die über einen Zugang zu einem Computer verfügen. Beispielsweise können Benutzer über ihren Computer beliebig oft versuchen, das Kennwort des Kontos *Administrator* herauszufinden. Es unterliegt nämlich nicht den Kennwortrichtlinien und kann auch nicht deaktiviert werden. Ist allerdings die Überwachungsrichtlinie ANMELDEVERSUCHE ÜBERWACHEN/FEHLGESCHLAGEN aktiviert, werden derartige Angriffe zumindest protokolliert. Sicherer ist es aber, wenn aus dem Anmeldenamen des Administratorkontos nicht auf die Funktion des entsprechenden Kontos geschlossen werden kann. Wird unter der Sicherheitsrichtlinie ein anderer Anmeldename eingegeben, wird er als Anmeldename des Kontos *Administrator* automatisch übernommen. Die Richtlinie sollte in einer Domänenumgebung aktiviert werden.

Beachten Sie, dass mit dem Anlegen eines **Donänenbenutzerkontos** der Benutzeranmeldename gesondert erfasst wird. Er ist nicht zu verwechseln mit dem Namen des Benutzerkontos, der im Verzeichnisbaum des Active Directory angezeigt wird (siehe Abbildung).



Benutzeranmeldename des Domänenbenutzerkontos Administrator

- **Anwender vor Ablauf des Kennwortes zum Ändern des Kennwortes auffordern**

  Standardmäßig wird der Benutzer 14 Tage vor Ablauf seines Kennwortes vom System aufgefordert, ein neues Kennwort zu vergeben. Mithilfe dieser Sicherheitsoption kann der Zeitraum verändert werden.

- **Letzten Benutzernamen nicht im Anmeldedialog anzeigen**

  Nachdem ein Benutzer seinen PC hochgefahren hat, erscheint im Anmeldefenster standardmäßig der Anmeldename des Benutzerkontos, das zuletzt am PC angemeldet war. Das Anzeigen des Anmeldenamens kann über die Aktivierung dieser Funktion verhindert werden. Dies ist z. B. dann von Vorteil, wenn mehrere Benutzer an einem PC arbeiten.

- **System sofort herunterfahren, wenn Sicherheitsüberprüfungen nicht protokolliert werden können**

  Diese Sicherheitsoption steht in Verbindung mit dem Sicherheitsprotokoll der Überwachungsrichtlinien. Bei der Verwaltung des Sicherheitsprotokolls muss festgelegt werden, welche Speicherkapazität es annehmen kann und wie Protokolleinträge zu bearbeiten sind, wenn die Speicherkapazität erreicht ist. Bei Erreichen der Speicherkapazität kann mit dieser Sicherheitsoption festgelegt werden, dass das System

automatisch herunterfährt. Diese schwerwiegende Maßnahme sollte jedoch gut bedacht werden. Es wird eher empfohlen, das Sicherheitsprotokoll so einzustellen, dass bei Erreichen der Kapazitätsgrenze ältere Einträge automatisch überschrieben werden. Wenn dann noch regelmäßig eine Auswertung des Protokolls stattfindet, sollten keine Einträge unerkannt bleiben.

- **Nachricht und Nachrichtentitel für Benutzer, die sich anmelden wollen**

  Mit diesen beiden Funktionen besteht die Möglichkeit, einen Nachrichtentext bzw. -titel mit dem Anmeldefenster zu verknüpfen. Sobald ein Benutzer die Tasten Strg+Alt+Entf betätigt, erscheint ein Fenster mit den in der Richtlinie hinterlegten Informationen. Mit der Taste OK gelangt man anschließend in das Anmeldefenster.

- **Auslagerungsdatei des virtuellen Arbeitsspeichers beim Herunterfahren des Systems löschen**

  Die Auslagerungsdatei PAGEFILE.SYS kann erhebliche Datenmengen enthalten, die auch nach dem Herunterfahren gespeichert bleiben. Die Datei ist im laufenden Betrieb von Windows 2000 ständig geöffnet, sodass ein Benutzer z. B. mit einem **Editor** den Inhalt nicht einsehen kann. Es gibt jedoch Möglichkeiten, die Datei auf einem anderen Wege für einen Angreifer zugänglich zu machen. Werden sehr sensible Daten auf dem System verarbeitet, die nach dem Abschluss der Datenverarbeitung vom System gelöscht werden, sollte auch die Auslagerungsdatei bereinigt werden.

  Ein weiterer Vorteil der Aktivierung dieser Sicherheitsfunktion ist, dass die **Fragmentierung** der Auslagerungsdatei eingeschränkt wird, weil sie sich nach jedem Löschen neu entfaltet und somit im unteren vorgegebenen Kapazitätsbereich bleibt (siehe Tz. 9.4.2 und Tz. 11.4).

- **Zugriff auf CD-ROM-Laufwerke/Diskettenlaufwerke auf lokal angemeldete Benutzer beschränken**

  Diese Sicherheitsoptionen unterstützen nicht die Deaktivierung des CD-ROM- und Diskettenlaufwerkes für den am Computer angemeldeten Benutzer. Die Deaktivierung erfolgt nur für Benutzer, die über das Netzwerk auf z. B. das CD-ROM-Laufwerk des eingeschränkten Computers zugreifen wollen.

Für die sichere Verwaltung der von einem Computer unterstützten Schnittstellen, wie z. B. die Disketten- und CD-ROM-Laufwerke, serielle und parallele Ports, USB-Anschlüsse usw., sollte ein professionelles Tool (z. B. DeviceLock, siehe Tz. 11.3) eingesetzt werden.

9.5 Sicherheitscheck

- *Beachten Sie, dass für die Umsetzung technischer **Sicherheitsmaßnahmen** unter Windows 2000 lokale und Active Directory-Richtlinien eingesetzt werden.*
- *Nach der Installation von Windows 2000 (Server oder Professional) bleiben die KONTO- und die ÜBERWACHUNGSRICHTLINIEN **deaktiviert**, während unter den SICHERHEITSOPTIONEN und den BENUTZERRECHTEN bereits viele Richtlinien aktiv sind.*
- *Überprüfen Sie die von Windows 2000 **aktivierten** Richtlinien und nehmen Sie ggf. Anpassungen vor.*
- *Planen und **dokumentieren** Sie den Einsatz der lokalen Sicherheitsrichtlinien, wenn auf dem Computer lokale Benutzerkonten eingerichtet werden sollen.*
- *Legen Sie fest, welche **Regeln** für die Vergabe von Kennwörtern zu beachten sind und setzen Sie diese mithilfe der Kontorichtlinien um.*
- *Aktivieren Sie die Überwachungsrichtlinie ANMELDEVERSUCHE ÜBERWACHEN FEHLGESCHLAGEN und legen Sie die **Zuständigkeit** für die Auswertung des Sicherheitsprotokolls fest (siehe Kapitel 10).*
- *Beachten Sie, dass für das Sicherheitsprotokoll eine ausreichende **Speicherkapazität** zur Verfügung steht und dass es regelmäßig ausgewertet wird.*
- *Weisen Sie das Benutzerrecht für den Zugriff auf das Sicherheitsprotokoll nach Möglichkeit einer Person **außerhalb** der IT-Abteilung zu.*
- *Machen Sie sich mit den **Benutzer- bzw. Systemrechten** vertraut. Mithilfe dieser Rechte können insbesondere administrative Aufgaben delegiert werden.*
- *Installieren Sie ein **Defragmentierungstool** für die in der Speicherkapazität anwachsenden Systemdateien (Pagefile.sys, siehe auch Kapitel 11).*
- *Machen Sie die Benutzer darauf aufmerksam, dass die Administratoren mithilfe der **Besitzübernahme** auf Ordner und Dateien zugreifen können.*
- *Beachten Sie, dass die Sicherheitsrichtlinien die Deaktivierung der Disketten-, CD-ROM-Laufwerke und sonstigen Schnittstellen **nicht** unterstützen.*

10 Active Directory-Gruppenrichtlinien

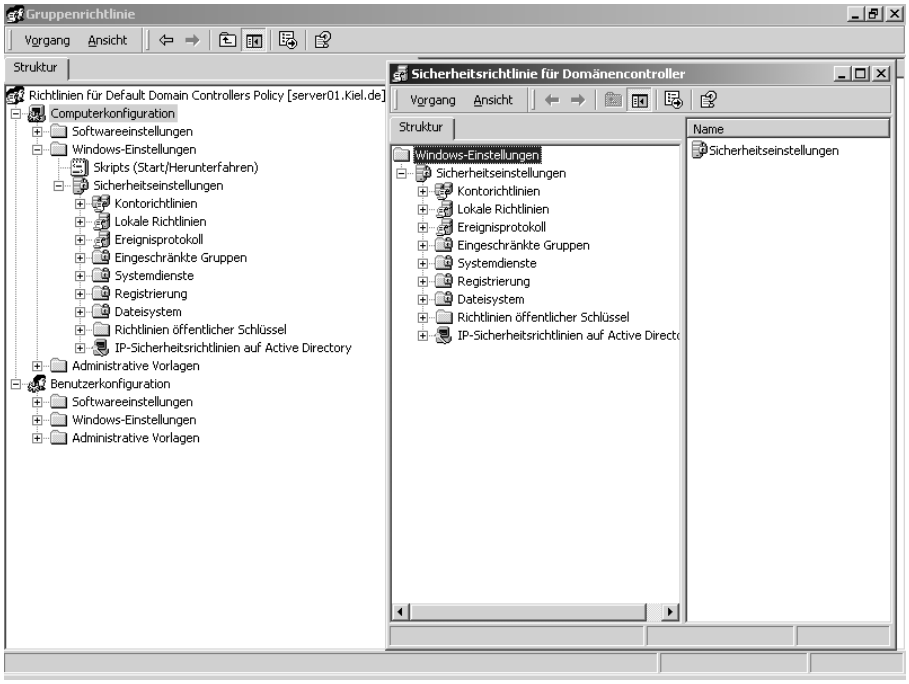
In diesem Kapitel erfahren Sie,

- welche Standard-Gruppenrichtlinien Windows 2000 unterstützt,
- mit welchen Verwaltungsprogrammen die Gruppenrichtlinien administriert werden,
- was bei der Funktionsweise der Gruppenrichtlinien zu beachten ist,
- wie das Zeitintervall für die Umsetzung der Gruppenrichtlinien geändert werden kann,
- in welcher Umgebung Windows NT Systemrichtlinien eingesetzt werden können,
- in welchen Dateistrukturen Gruppenrichtlinien gespeichert werden,
- mit welchen Vorlagen Gruppenrichtlinien erweitert werden können,
- welche Einstellungen in Standort-, Domänen-, Domänencontroller- und Organisationseinheiten-Gruppenrichtlinien vorgenommen werden sollten,
- was unter einer Gruppenrichtlinienfilterung zu verstehen ist und
- welche Tools für die Administration der Gruppenrichtlinien eingesetzt werden können.

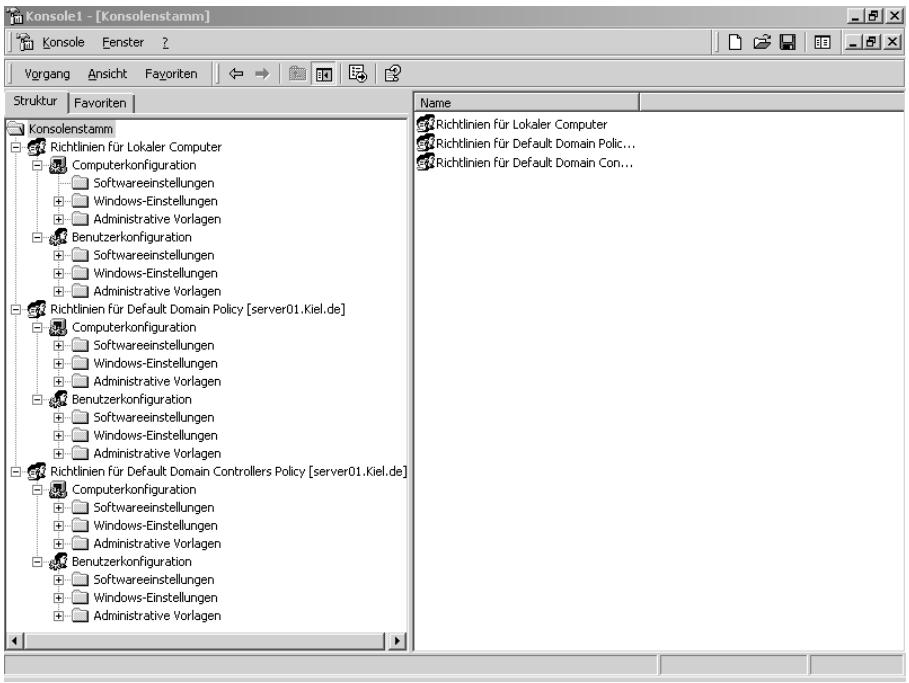
10.1 Gruppenrichtlinen-Strukturen

Wird ein Windows 2000 Server zu einem Domänencontroller hochgestuft, werden ihm neben den LOKALEN SICHERHEITSRICHTLINIEN zwei weitere für das Active Directory spezifische Sicherheitsrichtlinien zugeordnet. Dabei wird die Richtlinie DEFAULT DOMAIN POLICY mit dem Domänencontainer und die Richtlinie DEFAULT DOMAIN CONTROLLER mit dem Container Domänencontroller verknüpft. Active Directory-Sicherheitsrichtlinien werden auch als **Gruppenrichtlinien** bezeichnet. Sie werden als **Objekt** im Ordner \winnt\sysvol\sysvol\domänenname\policies> verwaltet und können einem Standort, einer Domäne und einer Organisationseinheit zugeordnet werden. Die vollständigen Gruppenrichtlinien werden im ***backUP*-Magazin Gruppenrichtlinien** erläutert. Aufgrund der Komplexität beschränkt sich dieses Kapitel auf die Beschreibung der Richtlinien, die für die **Sicherheit in einer Client/Serverumgebung** von Bedeutung sind. In der Desktopoberfläche des Domänencontrollers werden unter START-PROGRAMME-VERWALTUNG die Verwaltungsprogramme SICHERHEITSRICHTLINIEN FÜR DOMÄNEN (dompol.msc) und SICHERHEITSRICHTLINIEN FÜR DOMÄNENCONTROLLER (dcpol.msc) integriert. Wie bei den LOKALEN SICHERHEITSRICHTLINIEN

(secpol.msc) kann über den Aufruf dieser Verwaltungsprogramme (Managementkonsolen) nur der Knoten SICHERHEITSEINSTELLUNGEN administriert werden. Diese Verwaltungsprogramme stellen also nur jeweils einen **Ausschnitt** der entsprechenden Gruppenrichtlinie zur Verfügung (siehe Abbildung).



Richtlinien für Default Domain-Controllers – Ausschnitt Knoten Sicherheitseinstellung



Standard-Gruppenrichtlinien

Die Standard-Gruppenrichtlinien können aber auch vollständig als Snap-In in eine Managementkonsole integriert werden. Die Strukturen aller drei Gruppenrichtlinien sind identisch.Microsoft hat mit der Bereitstellung der verschiedenen Richtlinien-Verwaltungsprogramme und den unterschiedlichen Begriffsdefinitionen eher für Verwirrung gesorgt, als für eine logisch nachvollziehbare Handhabung. Verständlicher werden die Gruppenrichtlinien erst dann, wenn die genauen Strukturen und die Wirkungsweise am System begutachtet werden.

10.2 Funktionsweise der Gruppenrichtlinien

Mithilfe einer Gruppenrichtlinie lassen sich u. a. folgende Bereiche der Windows 2000-Funktionalität steuern:

- Zentrale Verwaltung der Softwareverteilung,
- Sicherheitseinstellungen (Konto-, Überwachungsrichtlinien, Benutzerrechte usw.),
- Skripteinbindung (Start und Herunterfahren, An- und Abmelden),
- Steuerung und Sicherheitseinstellung der Systemdienste,
- Zugriffsberechtigungen für Registry-Keys und NTFS-Verzeichnisse,
- Funktionseinschränkung des Clientdesktop,
- Zentralspeicherung der Benutzerprofilordner.

Darüber hinaus kann festgelegt werden, wie weiträumig eine Gruppenrichtlinie eingesetzt werden soll. Sie können sich auswirken auf:

Ebene	**Reihenfolge der Vererbung**
Lokaler Ebene,	1
Standortebene,	2
Domänenebene oder	3
Organisationseinheiten-Ebene.	4

Die *Lokale Richtlinie* eines Computers wird immer zuerst bearbeitet. *Active Directory-Gruppenrichtlinien* werden anschließend in der o.a. Reihenfolge ausgeführt. Das bedeutet, dass Active Directory-Gruppenrichtlinieneinstellungen **Vorrang** vor allen lokalen Einstellungen haben. Die Gruppenrichtlinien auf der Ebene der **Organisationseinheiten** sind deshalb am wichtigsten.

Mit der Ausführung der einzelnen Gruppenrichtlinien (Reihenfolge 1 – 4) werden nur **aktivierte Richtlinien** berücksichtigt. Ist z. B. in allen 4 Gruppenrichtlinien dieselbe Richtlinie mit unterschiedlichen Einstellungen aktiviert, wird zuerst die Lokale Richtlinie umgesetzt, danach die Standort-Richtlinie gefolgt von der Domänen-Richtlinie und der Organisationseinheiten-Richtlinie. Die zuletzt umgesetzte Richtlinie, in diesem Fall die OE-Richtlinie, überschreibt demnach die Einstellungen der vorherigen Richtlinien.

Beachten Sie, dass sich die Gruppenrichtlinien auf den Computer und die Benutzer unmittelbar auswirken. Fehlerhafte Einstellungen können zu Beeinträchtigungen des Systemverhaltens führen. Sie sollten deshalb zunächst auf einem Testsystem die von Ihnen geplanten Einstellungen vornehmen, bevor Sie sie auf das Produktionssystem übernehmen.

Bei dem Einsatz der Gruppenrichtlinien sind u. a. folgende **Besonderheiten** zu beachten:

1. Die Domänen-Gruppenrichtlinie hat in Bezug auf den Knoten SICHERHEITSEINSTELLUNGEN (Konto-, Lokale Richtlinien) Vorrang vor **allen** anderen Richtlinien.

2. Lokale**,** auf dem Client eingerichtete Benutzerkonten unterliegen ebenfalls dem Knoten SICHERHEITSEINSTELLUNGEN der Domänen-Gruppenrichtlinie. Alle anderen Active Directory-Gruppenrichtlinien wirken sich **nicht** auf lokale Benutzerkonten aus, sondern nur auf Domänenbenutzerkonten.

3. Der Knoten SICHERHEITSEINSTELLUNGEN findet in einer Organisationseinheiten-Gruppenrichtlinie keine Anwendung.

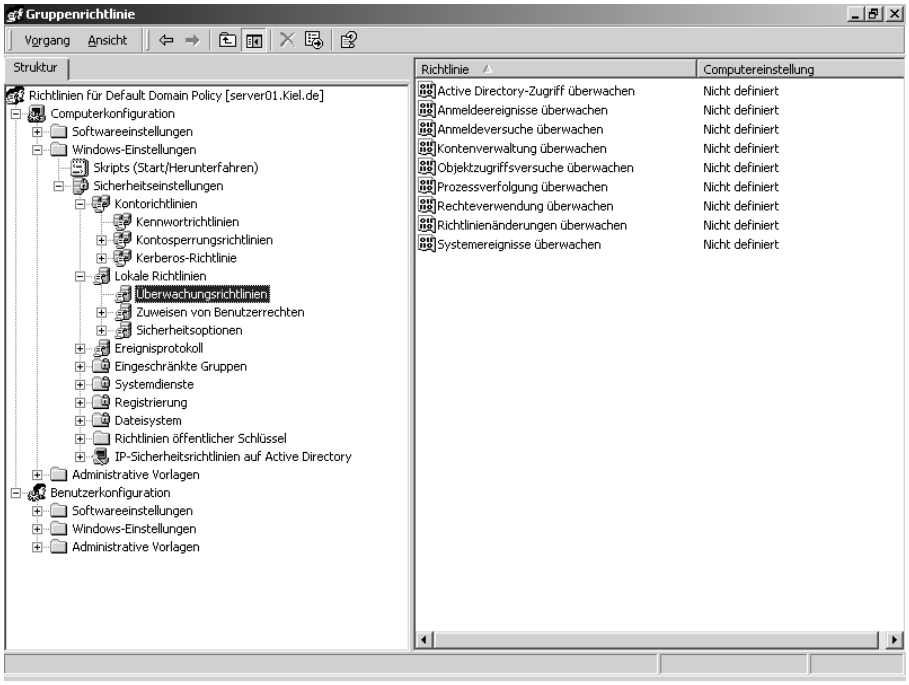
4. Die **Überwachungsrichtlinien** der Domänen- und der Domänencontroller-Gruppenrichtlinie kommen **beide** bei der Aktivierung zur Anwendung (siehe 5. und 6.).

5. Die Überwachungsrichtlinien der **Domänen-Gruppenrichtlinie** beziehen sich auf den Client. So werden z. B. fehlerhafte Anmeldeversuche oder überwachte lokale Objektzugriffe ausschließlich im Sicherheitsprotokoll des Client festgehalten. In dem Sicherheitsprotokoll auf dem Domänencontroller entstehen keine Protokolleinträge.

6. Die **Domänencontroller-Überwachungsrichtlinien** protokollieren hingegen Domänencontroller spezifische Aktivitäten im Sicherheitsprotokoll des Domänencontrollers. Hierzu gehören z. B. auch fehlerhafte Anmeldungen oder überwachte Objektzugriffe auf dem Domänencontroller, die von einem Client ausgehen.

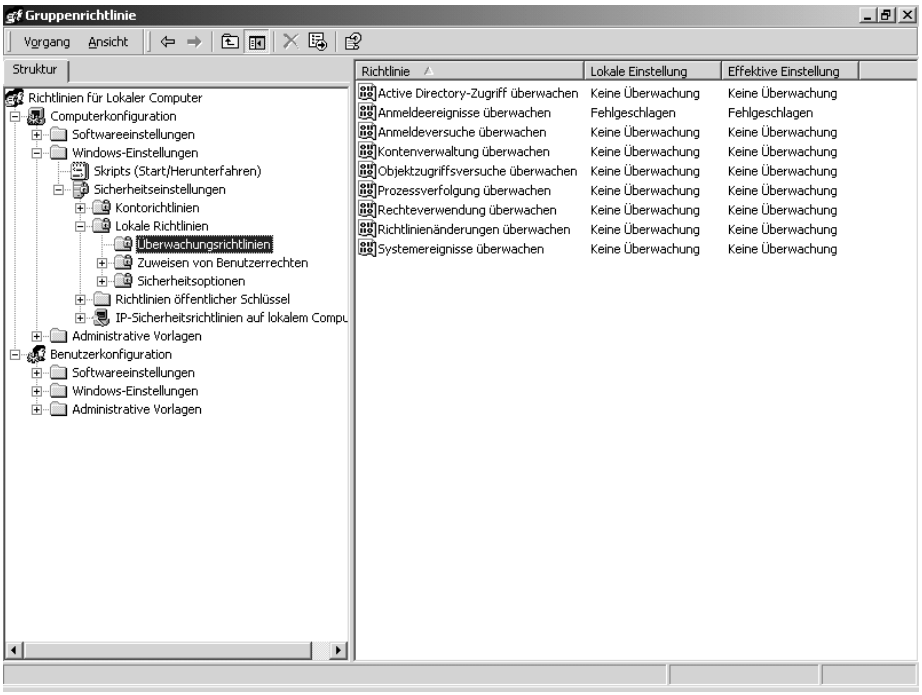
7. Die Aktivierung der Richtlinien unter dem Knoten BENUTZERKONFIGURATION in der Domänencontroller-Gruppenrichtlinie haben auf dem Client keine Auswirkungen.

8. Die **Domänen-Gruppenrichtlinie** bezieht den Domänencontroller mit ein. **Achtung,** Einschränkungen unter dem Knoten BENUTZERKONFIGURATION wirken sich auch auf das Administratorkonto aus.



Domänen-Gruppenrichtlinie auf dem Domänencontroller (Default Domain Policy)

- Aktivieren Sie die **Kontorichtlinien** in der Domänen-Gruppenrichtlinie.
- Aktivieren Sie **Überwachungsrichtlinien** in der Domänencontroller-Gruppenrichtlinie.
- Aktivieren Sie Richtlinien im Knoten **Benutzerkonfiguration** einer Organisationseinheiten-Gruppenrichtlinie für Einschränkungen der Desktopfunktionen auf dem Client.
- Aktivieren Sie **Lokale Gruppenrichtlinien** nur dann, wenn Sie auf dem Client lokale Benutzerkonten eingerichtet haben. **Achtung**, auch das lokale Administratorkonto unterliegt diesen Richtlinien.



Lokale Gruppenrichtlinie auf dem Client

Beispiel: Richtlinie ANMELDEEREIGNISSE ÜBERWACHEN

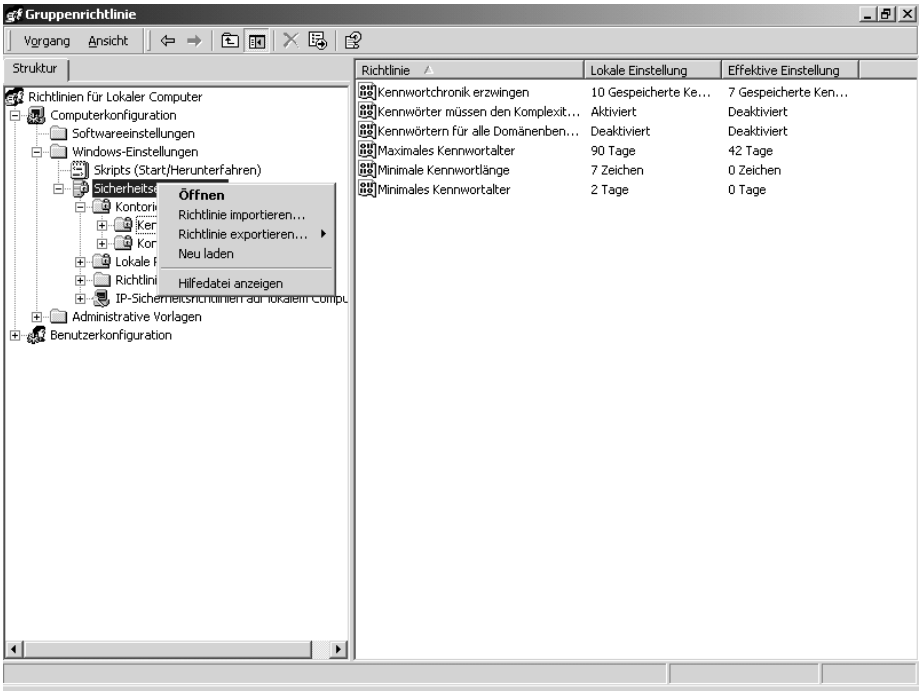
Reihenfolge der Richtlinie		**Einstellung**
1	Lokale Gruppenrichtlinie	Fehlgeschlagen
2	Domänen-Gruppenrichtlinie	Nicht definiert
=	Effektive Einstellung	Fehlgeschlagen

Die Richtlinie ANMELDEEREIGNISSE ÜBERWACHEN der Domänen-Gruppenrichtlinie überschreibt die entsprechende Richtlinie der Lokalen Gruppenrichtlinie **nicht**, weil sie nicht aktiviert und nicht explizit deaktiviert wurde. Sie hat den Status „Nicht definiert“.

Beispiel: Richtlinie KENNWORTCHRONIK ERZWINGEN

Reihenfolge der Richtlinie		**Einstellung**
1	Lokale Gruppenrichtlinie	10 gespeicherte Kennwörter
2	Domänen-Gruppenrichtlinie	7 gespeicherte Kennwörter
=	Effektive Einstellung	7 gespeicherte Kennwörter

Die Richtlinie KENNWORTCHRONIK ERZWINGEN der Domänen-Gruppenrichtlinie überschreibt die entsprechende Richtlinie der Lokalen Gruppenrichtlinie, weil sie aktiviert wurde.



Lokale Gruppenrichtlinie auf dem Client

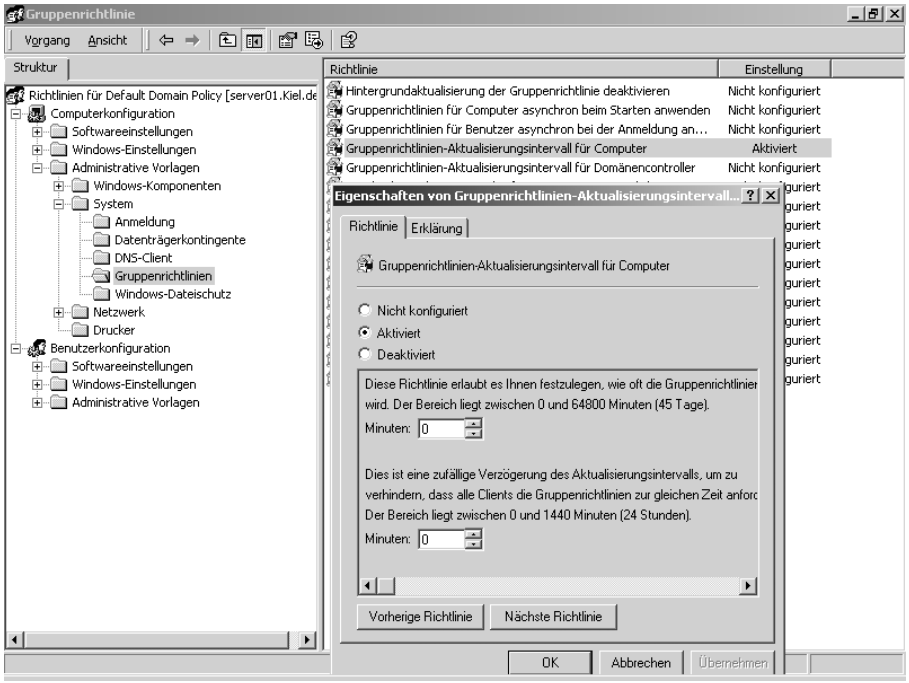
Die **Aktualisierung** der Anzeige der Gruppenrichtlinie in der Managementkonsole kann über die Option NEU LADEN des Kontextmenüs durchgeführt werden.

Gruppenrichtlinie in Bezug auf die Anzeige aktualisieren!

1. *Starten Sie die **Lokalen Gruppenrichtlinien** mit dem Programm GPEDIT.MSC.*
2. *Klicken Sie erst auf den Knoten WINDOWS-EINSTELLUNGEN und dann mit der rechten Maustaste auf den Knoten SICHERHEITSEINSTELLUNGEN.*
3. *Wählen Sie NEU LADEN und Gruppenrichtlinie wird in der Anzeige aktualisiert.*

Die Ausführung einer oder mehrerer Gruppenrichtlinien erfolgt grundsätzlich immer dann, wenn der Computer **neu gestartet** wird. Alle Einstellungen unter dem Knoten COMPUTERKONFIGURATION werden ausgeführt **bevor** das Anmeldemenü erscheint. Die unter dem Knoten BENUTZERKONFIGURATION enthaltenen Richtlinien werden unmittelbar **nach** der Anmeldung am System umgesetzt. Danach werden Konfigurationsveränderungen in den Gruppenrichtlinien alle **90 Minuten** mit einer zusätzlichen Verzögerung von bis zu **30 Minuten** aktualisiert. Eine Ausnahme stellt die Gruppenrichtlinie für Domänencontroller dar. Sie enthält als

Standardvorgabe für die Aktualisierung nur **5 Minuten**. Die Zeitintervalle für die Aktualisierung können aber auch in der Gruppenrichtlinie unter dem Knoten COMPUTERKONFIGURATION\ADMINISTRATIVEVORLAGEN\SYSTEM\GRUPPENRICHTLINIEN geändert werden. Die **standardmäßig** voreingestellten Zeitintervalle haben die Aufgabe, eine zu intensive Netzwerkkommunikation zwischen Domänencontroller und Client in Bezug auf die Sicherheitseinstellungen zu reduzieren.



Richtlinien für die Gruppenrichtlinie Defaul Domain Policy

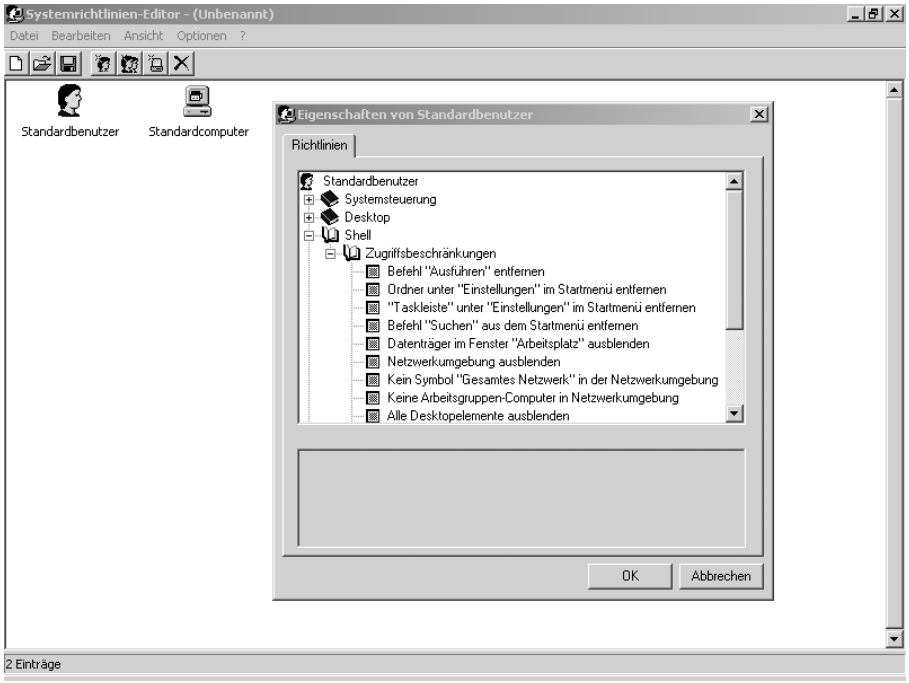
Für Testzwecke ist es empfehlenswert, die Aktualisierung und die Verzögerung auf 0 Minuten herabzusetzen, damit sich die Konfigurationsänderungen auf dem Client **sofort** auswirken.

- Beachten Sie, dass eine Veränderung der Aktualisierungsrichtlinie ebenfalls dem **voreingestelltem** Zeitintervall unterliegt. Das „neue“ Zeitintervall wird erst nach Ablauf des „alten“ Zeitintervalls aktiv.

- Starten Sie den Client deshalb neu, damit die Richtlinie sofort umgesetzt wird. Haben Sie das Aktualisierungsintervall und die Zeitverzögerung auf 0 Minuten gesetzt, werden künftig alle Konfigurationsänderungen in der entsprechenden Gruppenrichtlinie mit minimaler Verzögerung von bis zu ca. 30 Sekunden sofort aktiv bzw. auf den Client übertragen.

10.3 Windows NT-Systemrichtlinien

Windows NT Computer arbeiten mit den Systemrichtlinien, die mit POLEDIT.EXE erstellt und in der Datei NTCONFIG.POL auf dem Windows NT-Domänencontroller im Ordner <Stammverzeichnis:\winnt\system32\repl\import\scripts> mit der Freigabe NETLOGON gespeichert werden. In einer gemischten Umgebung mit Windows NT, 2000 und XP können NT-Systemrichtlinien und Active Directory-Gruppenrichtlinien eingesetzt werden. Windows 2000 Domänencontroller benutzen die Freigabe NETLOGON, die auf den Ordner <\Winnt\Sysvol\Sysvol\<Domänenname>\Scripts> umgeleitet wird. Um die Abwärtskompatibilität zu gewährleisten, werden unter Windows 2000 der Systemrichtlinien-Editor und ein vollständiger Satz ADM-Vorlagen unterstützt.



Windows NT-Systemrichtlinien auf einem Windows 2000 Domänencontroller

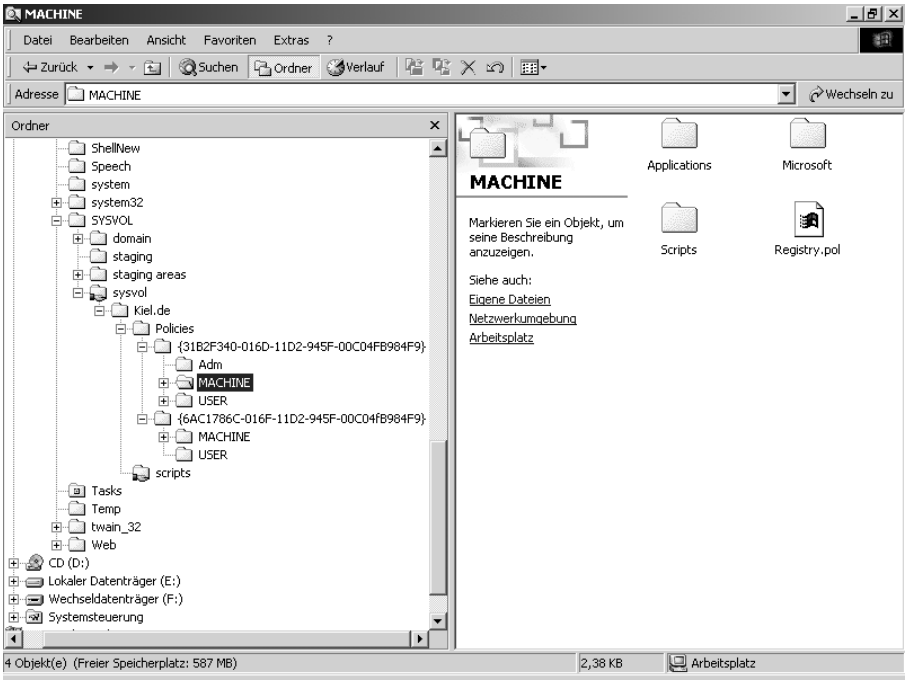
In einer gemischten Umgebung verarbeiten Windows 2000/XP Computer beim Starten zunächst die NT-Systemrichtlinien, dann die Lokalen Gruppenrichtlinien und im Anschluss die Active Directory-Gruppenrichtlinien.

Sie können die Verarbeitung der NT-Systemrichtlinien auf einem Windows 2000/XP Computer mit folgender Richtlinie ausschalten.

<Computerkonfiguration\Administrative Vorlagen\System\Gruppenrichtlinien\ Systemrichtlinie deaktivieren>

10.4 Gruppenrichtlinien-Dateistruktur

Die Gruppenrichtlinienobjekte werden auf dem Domänencontroller im Ordner <\winnt\sysvol\sysvol\<domänenname>\policies> gespeichert. Die Systeme zeichnen den Speicherort von Gruppenrichtlinienobjekten auf der Basis der GUID (Globally Unique Identifier – eine 128 Bit-Zahl, die die Eindeutigkeit garantiert) auf. Jeder Gruppenrichtlinienordner enthält mehrere Grundelemente:



Dateistruktur der Gruppenrichtlinien

- **Die Registry.pol-Datei:** Sie enthält die Registrierungseinträge, die vom Client heruntergeladen und auf die lokalen Registrierungseinträge im Speicher angewendet werden. Wenn Richtlinien sowohl Computern als auch Benutzern zugewiesen werden, wird jeder Satz von Richtlinien in einer eigenen Registry.pol-Datei gespeichert.

- **Der Ordner ADM:** Dieser Ordner enthält eine Kopie der administrativen Vorlagen (ADM-Dateien), anhand derer die Einträge in den Registry.pol-Dateien erzeugt werden. Diese Vorlagen werden von der Hauptvorlage im Ordner <Stammverzeichnis:\winnt\inf> des Domänencontrollers kopiert, auf dem die Richtlinie aktualisiert wird.

- **Der Ordner User:** Der Ordner enthält die Richtlinien, die auf die Registrierungseinträge des Schlüssels HKey_Current_User angewendet werden, wenn sich ein Benutzer anmeldet.

- **Der Ordner Machine:** Dieser Ordner enthält die Richtlinien, die auf die Registrierungseinträge im Schlüssel HKey_Local_Machine angewendet werden, wenn sich ein Computer anmeldet.

Gruppenrichtlinien lassen sich mit verschiedenen Containern/Organisationseinheiten verknüpfen, die dieselben Clients beeinflussen. Wenn ein Client Richtlinien aus mehreren Quellen herunterlädt, fügt er alle Registry.pol-Dateien für jeden Richtlinientyp (Benutzer- und Computerkonfiguration) in einer POL-Datei zusammen.

Die Registry.pol-Dateien für **Benutzereinstellungen** werden in der Datei NTUSER.POL zusammengeführt, die im Stammverzeichnis des Benutzerprofils im Ordner <Stammverzeichnis:\Dokumente und Einstellungen> gespeichert wird.

Die Registry.pol-Dateien für **Computereinstellungen** werden in einer Registry.pol-Datei kombiniert, die zusammen mit den lokalen Richtlinieneinstellungen im Ordner <Stammverzeichnis:\winnt\system32\GroupPolicy\Machine> gespeichert wird.

Die Registrierungseinträge, die in den Registry.pol-Dateien enthalten sind, werden addiert, falls keine Konflikte auftreten. Wenn ein Client verschiedene Richtlinien mit Einträgen herunterlädt, die **verschiedene** Registrierungsschlüssel aktualisieren, werden **alle** Registrierungseinträge angewendet. Wenn zwei oder mehr Registry.pol-Dateien Einträge enthalten, die **denselben** Registrierungsschlüssel betreffen, legt das System anhand einer **Hierarchie** (siehe Tz. 10.2) fest, welche Richtlinie den Vorrang hat.

Nachdem der Client an der Domäne angemeldet ist, sendet er alle **90 Minuten** eine Aktualisierungsanfrage für Gruppenrichtlinien an den Domänencontroller. Dieses Intervall lässt sich mit einer Richtlinie verändern (siehe Tz. 10.2). Mit dem Dienstprogramm SECEDIT.EXE können auch während des Betriebes Gruppenrichtlinien aktualisiert werden. Unter Windows Server 2003 XP und wird secedit.exe ersetzt durch gpupdate.exe.

secedit /refreshpolicy {machine_policy | user_policy}[/enforce]	
machine_policy	aktualisiert die Sicherheitseinstellungen für den lokalen Computer.
user_policy	aktualisiert die Sicherheitseinstellungen für das lokale Benutzerkonto des Benutzers, der aktuell an dem Computer angemeldet ist.
/enforce	aktualisiert die Systemsicherheit, auch wenn an den Einstellungen des Objekts Gruppenrichtlinie keine Änderungen vorgenommen wurden.

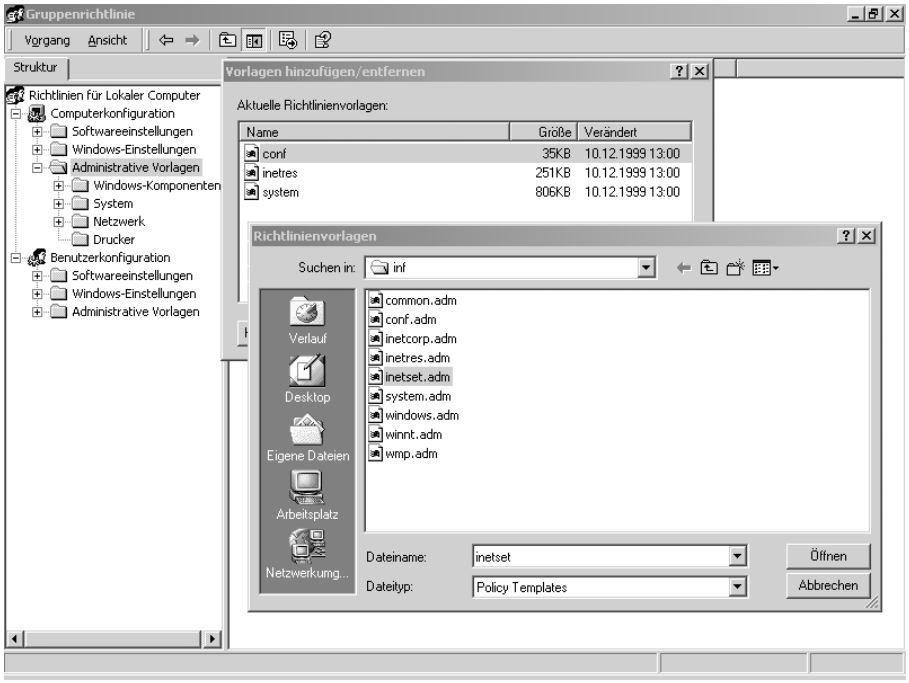
Die Registry.pol-Einträge, die die Richtlinien für die Computer- und die Benutzerkonfiguration definieren, stammen aus den administrativen Vorlagen. Diese ADM-Vorlagen haben dasselbe Format, wie die Systemrichtlinien.

Windows 2000 ist mit einem Satz von ADM-Vorlagen ausgestattet, die im Ordner <Stammverzeichnis:\winnt\inf\> gespeichert werden:

Vorlagen	**Beschreibung**
Winnt.adm	Systemrichtlinien für die Benutzeroberfläche von Windows NT 4.0
Windows.adm	Systemrichtlinien für die Benutzeroberfläche von Windows 9.x
Common.adm	Systemrichtlinien für die Benutzeroberfläche, die auf beiden Plattformen eingesetzt werden können.
conf.adm	eine beschränkte Anzahl von Explorer-Shell-Beschränkungen, mit denen das Aussehen von Active Desktop gesteuert wird (wird standardmäßig geladen).
Inetres.adm	Internet Explorer-Richtlinien, die Windows-Komponenten, wie z. B. der Internet Explorer, die Systemsteuerung und die Offlinedateien beeinflussen (wird standardmäßig geladen).
System.adm	umfassender Satz an Systembeschränkungen. Richtlinien für das Startmenü, die Taskleiste, den Desktop, die Systemsteuerung, das Netzwerk sowie Systemeinstellungen für An- und Abmeldung, Gruppenrichtlinien und Richtlinien für die Windows-Komponenten, wie z. B. Explorer, MMC, Taskplaner und Windows-Installer (wird standardmäßig geladen).
Inetset.adm	zusätzliche Richtlinien für den Internet-Explorer
Inetcorp.adm	spezielle Steuerelemente für Internet-Explorer-Sprachen, Beschränkungen für DFÜ-Netzwerke und Zwischenspeicher.
Conf.adm	Richtlinien für NetMeeting
Wmp.adm	Windows Media Player-Richtlinien

Die ersten drei ADM-Dateien dienen dazu, die Abwärtskompatibilität zu Windows NT 4 zu gewährleisten. Der Gruppenrichtlinien-Editor setzt standardmäßig die drei ADM-Vorlagen

SYSTEM.ADM, INETRES.ADM und CONF.ADM ein. Wenn der Gruppenrichtlinieneditor geladen wird, kopiert er ausgewählte Vorlagen aus dem Ordner <Stammverzeichnis:\winnt\inf> in den Richtlinienordner <\winnt\sysvol\sysvol\.....\adm>.



Vorlagen über den Gruppenrichtlinieneditor hinzufügen

ADM-Vorlage zu einer Lokalen Gruppenrichtlinie hinzufügen!

1. *Starten Sie über AUSFÜHREN den Gruppenrichtlinieneditor, indem Sie* `gpedit.msc` *eingeben.*

2. *Klicken Sie mit der rechten Maustaste auf den Knoten ADMINISTRATIVE VORLAGEN und wählen Sie VORLAGEN HINZUFÜGEN/ENTFERNEN.*

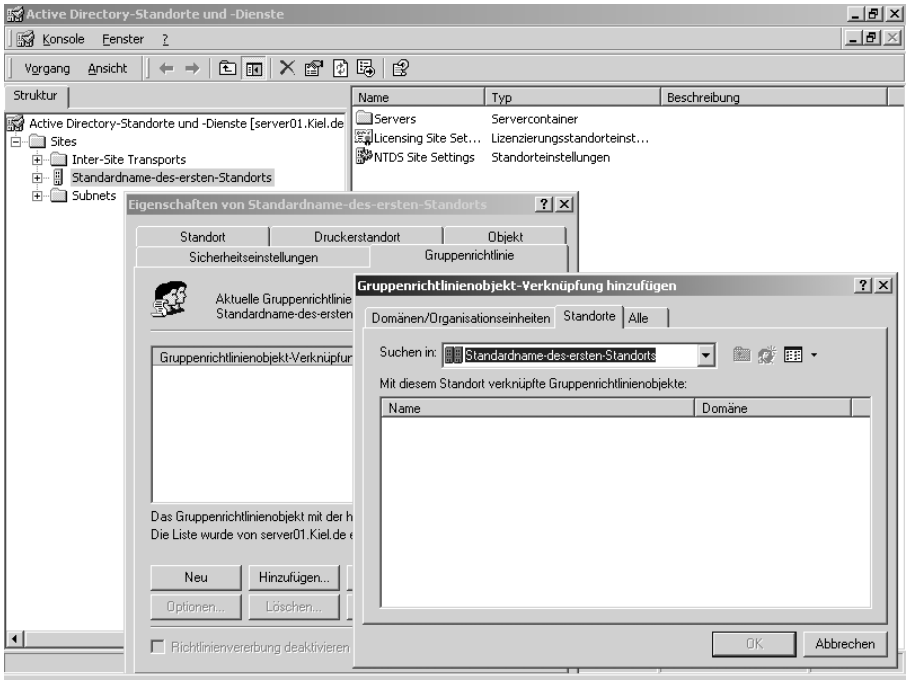
3. *Es öffnet sich ein Fenster mit den bereits geladenen Vorlagen. Klicken Sie auf HINZUFÜGEN und wählen Sie in dem nächsten Fenster mit Doppelklick eine Vorlage aus.*

4. *Die Vorlage wird nun in den Gruppenrichtlinienordner <\winnt\sysvol\sysvol\.....\adm> kopiert. Schließen Sie das Fenster und beenden Sie den Gruppenrichtlinieneditor.*

5. *Starten Sie den Gruppenrichtlinieneditor erneut. Die neue Vorlage ist jetzt aktiv.*

10.5 Standort-Gruppenrichtlinie

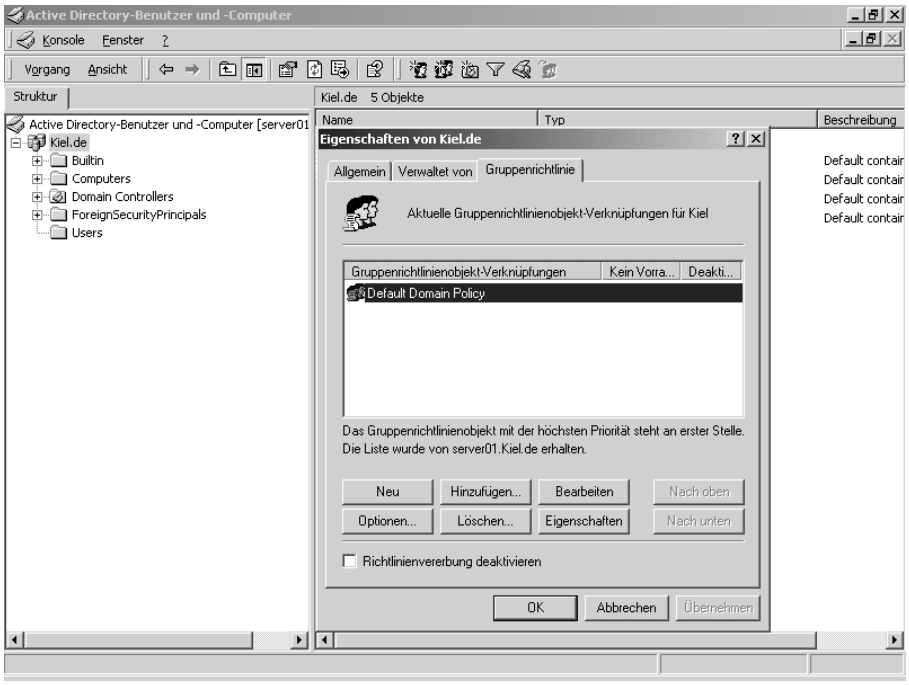
Die Grenzen für einen Standort werden durch die WAN- und nicht durch die Domänentopologie vorgegeben. Deshalb kann es zu ablauforganisatorischen Problemen führen, wenn eine Gruppenrichtlinie mit einem Standort verknüpft wird. Standortgruppenrichtlinien sollten ggf. zur Verteilung von Netzwerkkonfigurationen eingesetzt werden, (z. B. RAS-Richtlinien). Eine Standort-Gruppenrichtlinie wird über das Verwaltungsprogramm ACTIVE DIRECTORY-STANDORTE UND –DIENSTE aufgerufen.



Standort-Gruppenrichtlinie hinzufügen

10.6 Domänen-Gruppenrichtlinie

Eine Domänen-Gruppenrichtlinie wird auf **alle Benutzer und alle Computer** in der Domäne angewendet. Auf dieser Ebene sollten grundsätzliche Sicherheitsmaßnahmen umgesetzt werden, die für die gesamte Domäne bzw. Organisation gelten. Standardmäßig wird die Gruppenrichtlinie DEFAULT DOMAIN POLICY unterstützt. Sie wird über das Verwaltungsprogramm ACTIVE DIRECTORY-BENUTZER UND -COMPUTER aufgerufen.



Domänen-Gruppenrichtlinie bearbeiten

Die Domänen-Gruppenrichtlinie aufrufen!

1. *Rufen Sie über START-PROGRAMME-VERWALTUNG das Snap-In ACTIVE DIRECTORY- BENUTZER UND -COMPUTER auf.*

2. *Klicken Sie mit der rechten Maustaste auf den Namen der Domäne und wählen Sie EIGENSCHAFTEN.*

3. *Wechseln Sie zu der Registerkarte Gruppenrichtlinien und klicken Sie zur Bearbeitung der Gruppenrichtlinie auf BEARBEITEN, zur Erstellung einer neuen Gruppenrichtlinie auf NEU und zum Löschen einer bestehenden Gruppenrichtlinie auf LÖSCHEN.*

10.6.1 Kennwortrichtlinien

In Kapitel 9 werden die Kennwortrichtlinien für einen Einzelplatz-PC umfassend erläutert. Es sollten in einer Domänenumgebung folgende Einstellungen gewählt werden:

Richtlinie	**Empfohlene Einstellung**
Kennwortchronik erzwingen	10

Kennwörter müssen den Komplexitätsanforderungen entsprechen	aktiviert
Kennwörter für alle Domänenbenutzer mit umkehrbarer Verschlüsselung speichern	deaktiviert
Maximales Kennwortalter	max. 90
Minimale Kennwortlänge	7
Minimales Kennwortalter	3

10.6.2 Kontosperrungsrichtlinien

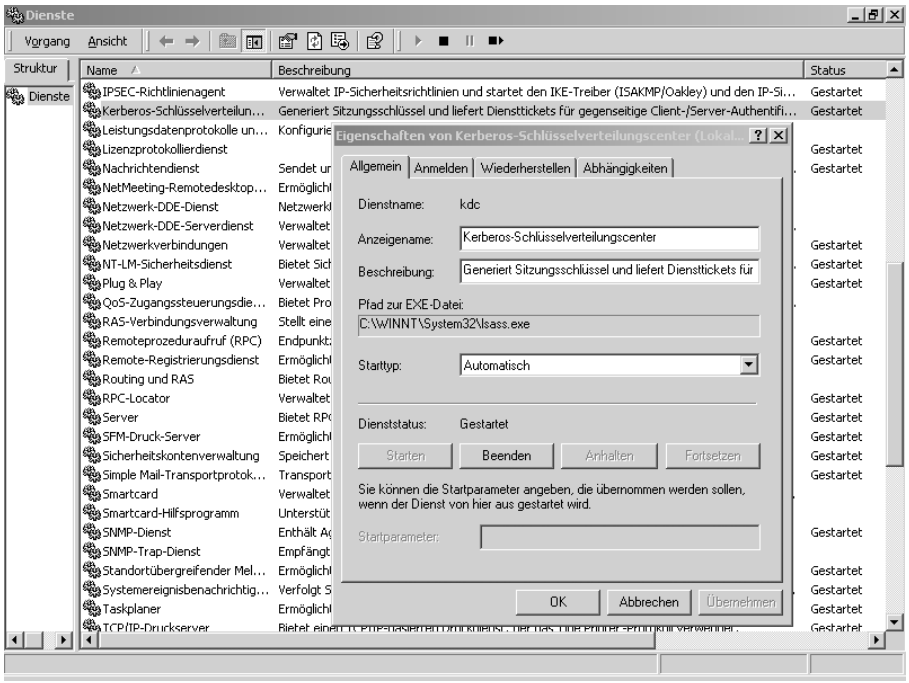
Auch die Kontosperrungsrichtlinien (siehe Kapitel 9) haben in einer Domänenumgebung eine zentrale Bedeutung. Sie sollten wie folgt umgesetzt werden:

Richtlinie	**Empfohlene Einstellung**
Kontosperrungsschwelle	3
Kontosperrdauer	0
Kontosperrungszähler zurücksetzen nach	30

10.6.3 Kerberos-Richtlinie

Die wesentliche Funktion der **Kerberos-Authentifizierung** besteht in der Verlagerung der **Identitätsprüfung** eines Benutzers auf einen zentralen Dienst. Dieser verwaltet in einer Datenbank alle Ressourcen (z. B. Benutzer- u. Computerkonten, Netzwerkdienste) mit zugewiesenen Schlüsseln. Meldet sich ein Benutzer am PC an, wird eine Anforderung für ein so genanntes Benutzerticket an den Kerberos-Dienst gesendet. Dieser vergleicht den Absender mit den Angaben seiner **Datenbank** und erstellt, sofern er ihn findet, ein Dienstticket. Das Dienstticket wird mit dem Schlüssel des Benutzers verschlüsselt an den Client gesendet. Das Anmeldeprogramm entschlüsselt das Dienstticket mithilfe des Benutzer-Key, den es aus dem Passwort des Benutzers errechnet. Innerhalb eines definierten zeitlichen Rahmens kann das Dienstticket wiederverwendet werden. Danach ist eine erneute

Anforderung beim Kerberos-Dienst notwendig. Des Weiteren wird durch einen Zeitstempel sichergestellt, dass ein einmal ausgestelltes Dienstticket nicht mehrfach verwendet werden kann. Mit den Kerberos-Richtlinien können die **Parameter** für den Authentifizierungsprozess administriert werden.



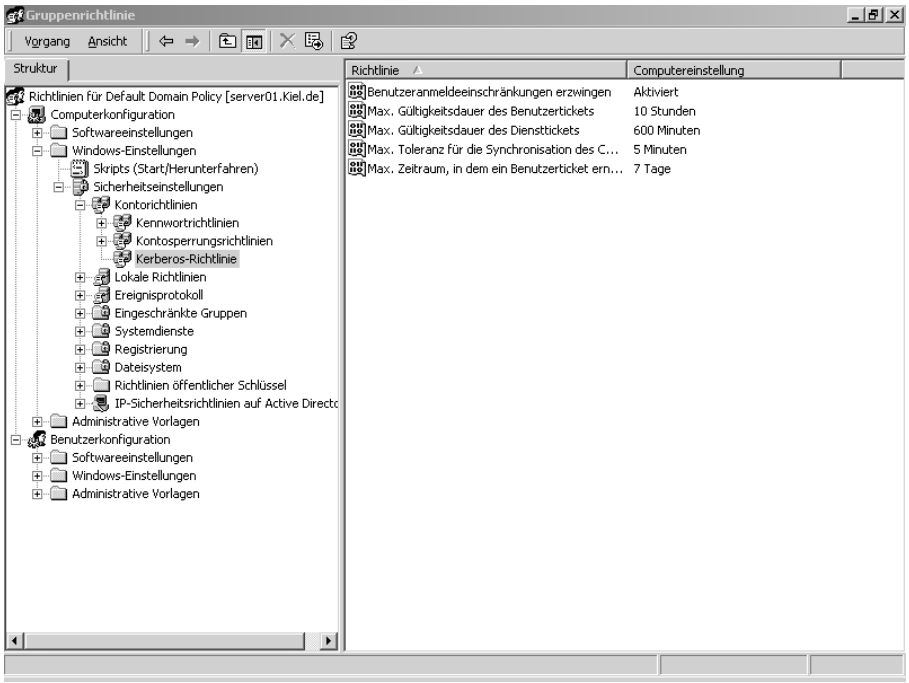
Kerberos-Dienst

Benutzeranmeldeeinschränkungen erzwingen
Standard-Einstellung: Aktiviert
Wird diese Option aktiviert, prüft der Kerberos Dienst bei jeder Anforderung eines Dienst-tickets, ob für das entsprechende Benutzerkonto auf dem Zielcomputer Anmelde-einschränkungen vorliegen. Diese Prüfung soll auch sicherstellen, dass das anfordernde Konto noch gültig ist. Die Prüfung ist optional, da der zusätzliche Schritt Zeit kostet und den Netz-werkzugriff auf Dienste verlangsamen kann.

Max. Gültigkeitsdauer des Benutzertickets
Standard-Einstellung: 10 Stunden
Nach Ablauf der Gültigkeitsdauer muss das Benutzerticket und alle darauf ausgestellten Diensttickets erneut werden.

Max. Gültigkeitsdauer des Diensttickets
Standard-Einstellung: 600 Min.
Dieser Wert muss größer als 10 Minuten und kleiner oder gleich der Gültigkeitsdauer des Benutzertickets sein. Die Diensttickets müssen grundsätzlich immer vor bzw. mit dem Benutzerticket ablaufen, um Inkonsistenzen bei den Berechtigungen zu vermeiden. Falsche Angaben werden automatisch korrigiert bzw. angepasst.

Max. Toleranz für die Synchronisation des Computertakts
Standard-Einstellung: 5 Minuten
Gibt die maximale Zeitdifferenz in Minuten an, die zwischen der Uhr des Clients und des Servers bestehen darf. Ist die Toleranzschwelle überschritten, kann der Client sich nicht mehr am Domänencontroller anmelden bzw. keine Netzwerkressourcen mehr nutzen.



Kerberos-Richtlinien (Standardeinstellungen)

Max. Zeitraum, in dem ein Benutzerticket erneuert werden kann
Standard-Einstellung: 7 Tage
Die Erneuerung des Benutzertickets – standardmäßig nach 10 Stunden – kann nur innerhalb des angegebenen Zeitraums durchgeführt werden. Danach ist eine erneute Anmeldung durch den Benutzer erforderlich.

Das Kerberos-Authentifizierungsprotokoll wird nur bei der Domänenanmeldung verwendet. Die LOKALEN SICHERHEITSRICHTLINIEN, die für die lokale Benutzeranmeldung maßgeblich sind, enthalten deshalb die Kerberos-Richtlinien nicht.

Neben der Authentifizierung wird das Kerberos-Protokoll auch zur Rechteverwaltung eingesetzt. Das Dienstticket enthält zusätzlich die Security Identifiers (SID) des Benutzers, mit denen die Befugnisse des Benutzers feststellbar sind.

Schlüsselverteilungscenter (Kerberos Dienst)

Das Schlüsselverteilungscenter (Key Distribution Center, KDC) beinhaltet den Authentifizierungsserver (AS) und den Ticketerteilungsdienst (TGS). Beide Funktionen werden standardmäßig auf dem Domänencontroller ausgeführt. Der Ticketverteilungsdienst verteilt Dienst-tickets an Clients, die sich mit Servern im Netzwerk verbinden möchten. Um jedoch ein Dienstticket zu erhalten, benötigt der Client vom Authentifizierungsserver zunächst ein so genanntes Benutzerticket (Ticket Granting Ticket, TGT). **Dienstticket**

Das Dienstticket beinhaltet die Identität des Benutzers, einen Sitzungsschlüssel, die Erstellungs- sowie die Ablaufzeit. Mithilfe des Diensttickets kann sich ein Client an einem Server authentifizieren. Es ist verschlüsselt und kann nur vom Zielserver entschlüsselt werden.

Benutzertickets
Mit dem Benutzerticket wird vom Authentifizierungsserver ein Dienstticket und ein Sitzungsschlüssel angefordert.

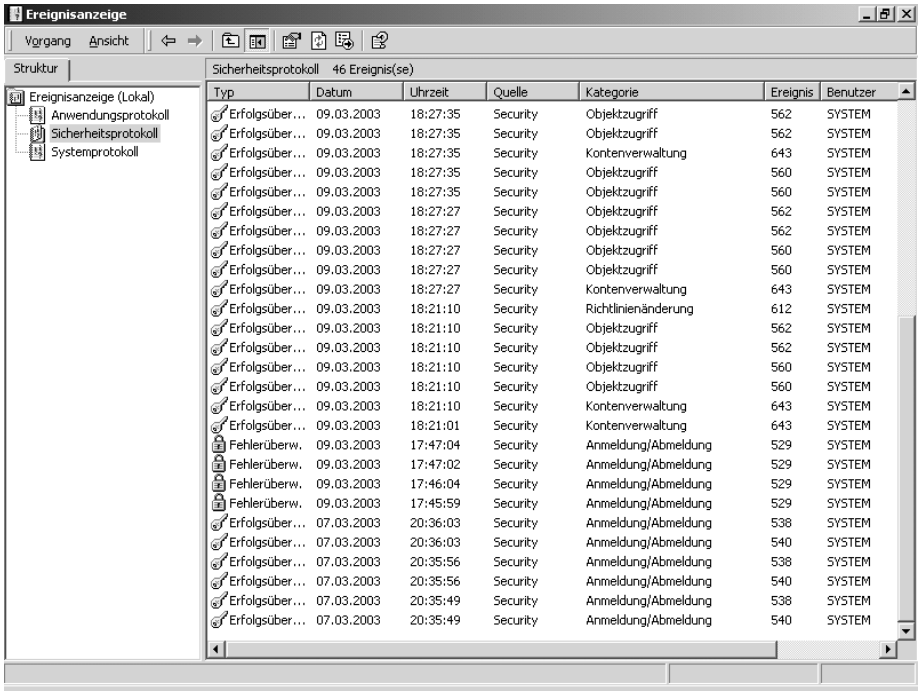
Sitzungsschlüssel

Der Sitzungsschlüssel dient zur Verschlüsselung des Authentifizierungsprozesses und wird zwischen Client und Server ausgetauscht.

10.6.4 Überwachungsrichtlinien

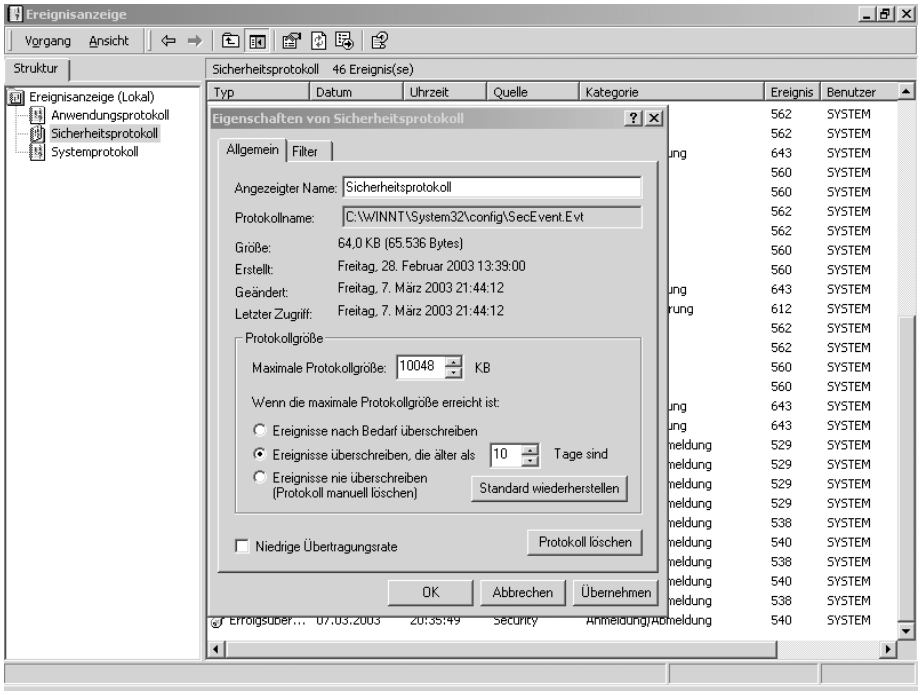
Mithilfe der Überwachungsrichtlinien können erfolgreiche oder fehlgeschlagene Aktivitäten der Benutzer und der Administratoren (begrenzt) protokolliert werden. Standardmäßig sind nach der Installation von Windows 2000 die Überwachungsrichtlinien **deaktiviert**. Die Auswahl der zu überwachenden Ereignisse sollte sorgfältig geplant werden. Die Aktivierung der Überwachungsrichtlinien setzt jedoch voraus, dass eine **Zuständigkeit** für die Auswertung der zahlreich entstehenden Protokolleinträge geschaffen wird. Da insbesondere auch **administrative** Aktivitäten, wie z. B. die Kontenverwaltung oder Active Directory Zugriffe, überwacht werden können, sollte die Zuständigkeit für die Auswertung der Protokolleinträge **nicht** im Bereich der Administration liegen.

Die Protokolleinträge können über die Ereignisanzeige unter SICHERHEITSPROTOKOLL ausgewertet und verwaltet werden. Da sich die Gruppenrichtlinie DEFAULT DOMAIN POLICY auf Clients bezieht, werden nur Aktivitäten protokolliert, die vom Client ausgehen. Die Protokolleinträge werden in der Ereignisanzeige im Sicherheitsprotokoll des **entsprechenden Clients** verwaltet. Sollen z. B. Aktvitäten der Administratoren auf dem **Domänencontroller** protokolliert werden, sind die entsprechenden Richtlinien der Gruppenrichtlinie DEFAULT DOMAIN CONTROLLERS POLICY zu aktivieren (siehe Tz. 10.7).



Ereignisanzeige, Sicherheitsprotokoll auf dem Client

Mit der Aktivierung der Überwachungsrichtlinien muss auf dem **Client** bestimmt werden, wie das Sicherheitsprotokoll verwaltet werden soll. Es empfiehlt sich, die standardmäßige Kapazitätgrenze erheblich anzuheben und nach Erreichen ein **Überschreiben** der ältesten Einträge zuzulassen. Durch eine **regelmäßige Auswertung** sollte gewährleistet werden, dass keine Protokolleinträge ungeprüft vom System überschrieben werden.



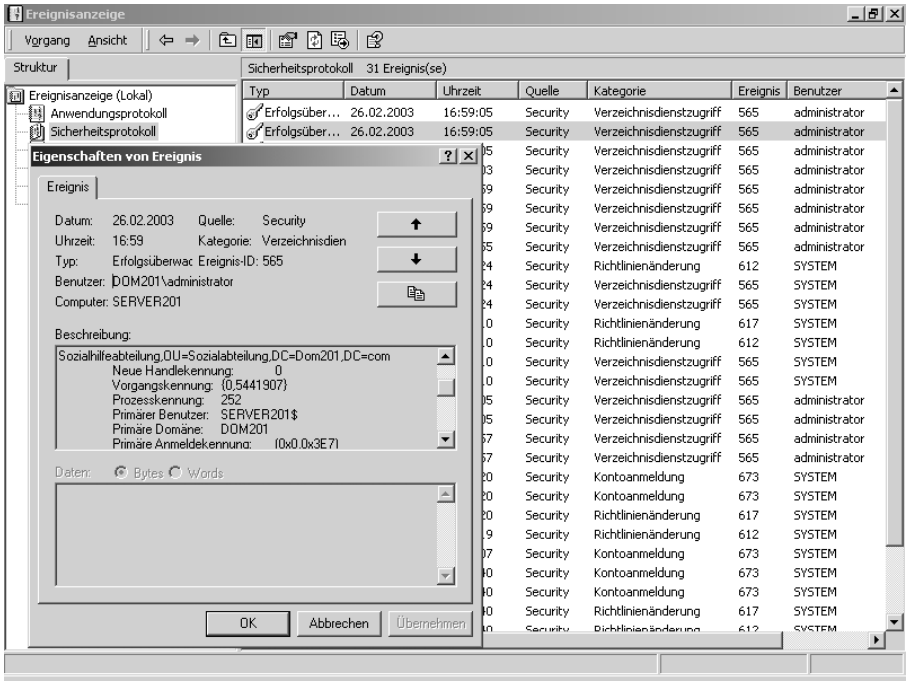
Eigenschaften des Sicherheitsprotokolls auf dem Client

10.7 Domänencontroller-Gruppenrichtlinie

Eine Domänencontroller-Gruppenrichtlinie wirkt sich unmittelbar auf den **Domänencontroller** aus. Aktivitäten auf dem Domänencontroller, wie z. B. Active Directory-Zugriffe, die Benutzer- und Gruppenkontenverwaltung, Richtlinienänderungen, Objektzugriffe auf Ordner und Dateien des Domänencontrollers sowie vom Client ausgehende Anmeldeversuche können im Sicherheitsprotokoll des **Domänencontrollers** protokolliert werden.

Wie unter Tz. 10.6.4 beschrieben, sind vor der Aktivierung der Überwachungsrichtlinien die Eigenschaften des Sicherheitsprotokolls des Domänencontrollers festzulegen.Die Gruppenrichtlinie Default Domain Controllers Policy wird über das Verwaltungsprogramm Active Directory Benutzer und –Computer unter dem Knoten Domain Controllers aufgerufen.

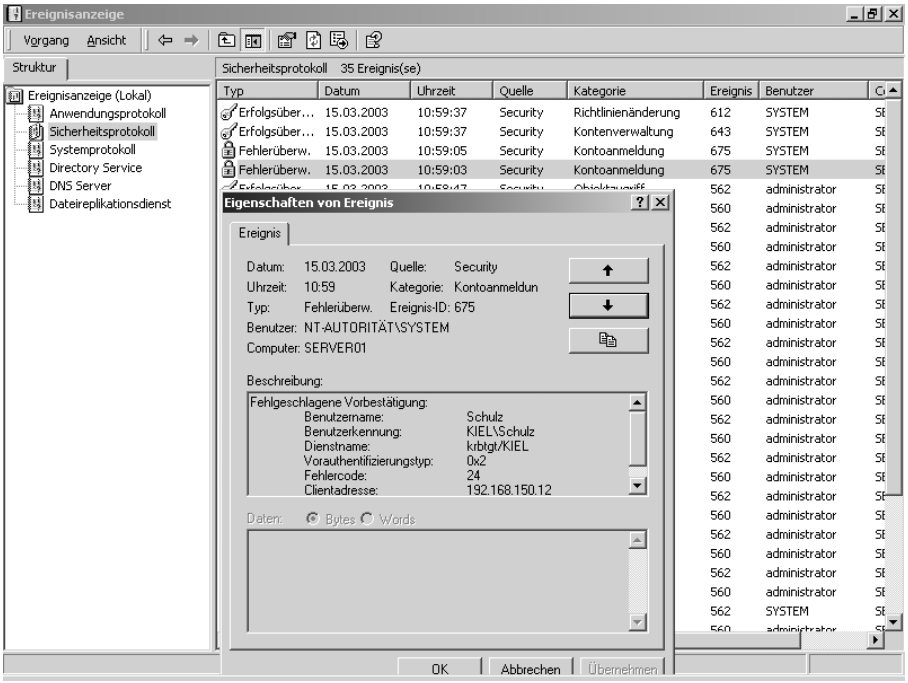
Active Directory-Zugriff überwachen
Empfohlene Einstellung: Keine Überwachung
Kategorie: Verzeichnisdienstzugriff
Über diese Richtlinie werden sämtliche Zugriffe auf das Active Directory überwacht. Es werden lesende Zugriff auf die Objekte im Active Directory protokolliert, so dass dadurch zahlreiche Protokolleinträge im Sicherheitsprotokoll entstehen. Die Aktivierung dieser Überwachungsrichtlinie kann nicht auf einzelne Benutzerkonten begrenzt werden. Darüber hinaus sagen die Protokolleinträge nicht viel über die administrativen Aktivtäten aus. Diese Richtlinie sollte nur im begründeten Einzelfall, z. B. zur Aufklärung von Systemfehlern, aktiviert werden.



Ereignisanzeige – Sicherheitsprotokoll auf dem DC, Active Directory-Zugriff überwachen

Anmeldeereignisse überwachen
Empfohlene Einstellung: Keine Überwachung
Kategorie: Anmeldung/Abmeldung
Es werden An- und Abmeldungen an der Konsole überwacht. Im Ereignisprotokoll werden u. a. der Name des Benutzerkontos und der Name der Arbeitsstation gespeichert, so dass

beispielsweise festgestellt werden kann, von welcher Arbeitsstation fehlgeschlagene Anmeldungen durchgeführt wurden. Diese Erreignise werden auch von der Richtlinie ANMELDEVERSUCHE ÜBERWACHEN protokolliert.



Ereignisanzeige – Sicherheitsprotokoll auf dem DC, Anmeldeversuche überwachen

Anmeldeversuche überwachen
Empfohlene Einstellung: Fehlgeschlagen
Kategorie: Kontoanmeldung
Mithilfe dieser Richtlinien können An- und Abmeldungen an der Konsole und An- und Abmeldungen über den Netzwerkzugriff von einem anderen PC überwacht werden. Im Ereignisprotokoll werden der Name des Kontos und der Name der Arbeitsstation festgehalten. Da diese Richtlinie weitgehender ist als die Richtlinie ANMELDEEREIGNISSE ÜBERWACHEN, reicht es aus, wenn nur diese Richtlinie aktiviert wird.

Kontenverwaltung überwachen
Empfohlene Einstellung: Erfolgreich, Fehlgeschlagen
Kategorie: Kontenverwaltung

Mit KONTOVERWALTUNG ÜBERWACHEN kann je nach Funktion des Systems die Administration der Domänenbenutzerkonten im Active Directory oder die Administration der lokalen Benutzerkonten protokolliert werden. Es wird allerdings nicht protokolliert,welche Änderungen an einem Konto durchgeführt wurden.. Es werden nur der Name des geänderten Benutzerkontos und der Name des Administrations-Benutzerkontos festgehalten.

Objektzugriffsversuche überwachen

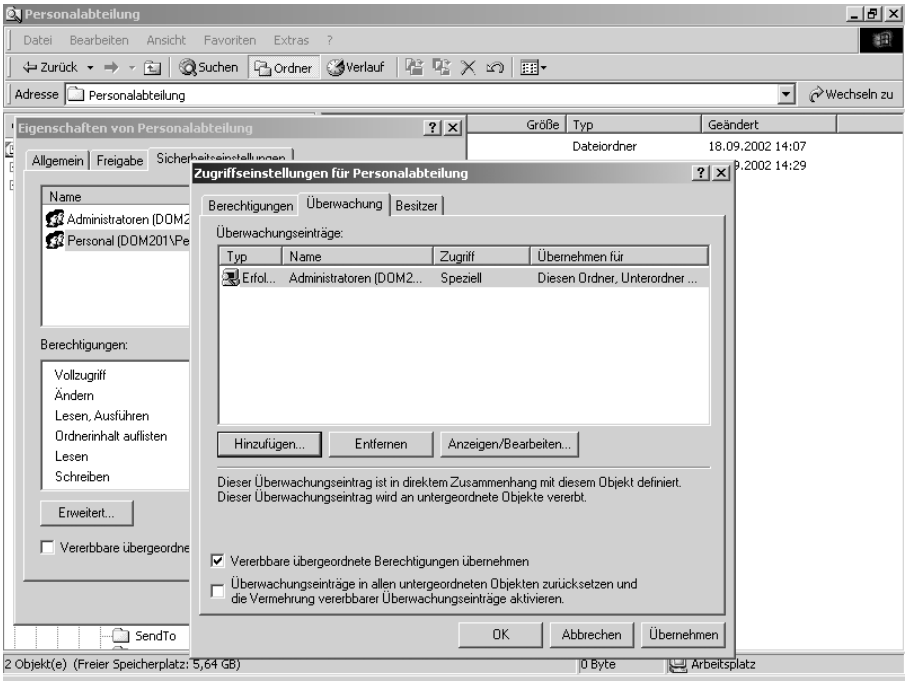
Empfohlene Einstellung: Erfolgreich, Fehlgeschlagen

Kategorie: Objektzugriff

Der Zugriff auf Objekte, wie z. B. Dateien und Ordner, kann überwacht werden. Der Einsatz dieser Richtlinie ist dann von Bedeutung, wenn über NTFS-Berechtigungen keine Datenabschottung gewährleistet werden kann. Das liegt insbesondere bei den administrativen Benutzerkonten vor. Die Administratoren haben aufgrund ihrer umfassenden Befugnisse häufig Vollzugriff auf alle Daten.Durch den Einsatz der Richtlinie OBJEKTZUGRIFFSVERSUCHE ÜBERWACHEN kann sichergestellt werden, dass auch Zugriffe von Administratoren auf Ordner und Dateien protokolliert werden. In der Ereignisanzeige wird unter der Kategorie OBJEKTZUGRIFF angezeigt, welches Benutzerkonto auf welches Objekt zugegriffen hat.

Der entsprechende Administrator kann zwar im Falle eines unberechtigten Dateizugriffs auf die Ereignisanzeige zugreifen, ist aber nicht in der Lage, das Sicherheitsprotokoll zu manipulieren. Er kann lediglich das gesamte Protokoll löschen. Das führt aber zu einem erneuten Eintrag, der den Namen des Benutzerkontos enthält, unter dem die Löschung durchgeführt wurde. Was dem Administrator dazu veranlasst hat, das Sicherheitsprotokoll zu löschen, muss dann plausibel von ihm begründet werden. Zu berücksichtigen ist weiterhin, dass der Administrator die Überwachung nicht unbemerkt umgehen kann, indem er sie vor dem Zugriff ausschaltet und hinterher wieder einschaltet. Deshalb ist die Richtlinie RICHTLINIENVERÄNDERUNGEN ÜBERWACHEN zu aktivieren.

Die Aktivierung dieser Richtlinie ist verbunden mit der Bestimmung der entsprechenden Dateien und/oder Ordner, die überwacht werden sollen. Unter den SICHERHEITSEINSTELLUNGEN eines Objektes (z. B. Datei oder Ordner) kann über die Option ERWEITERT die Registerkarte ÜBERWACHUNG ausgewählt werden. Es lassen sich dann die zu überwachenden Benutzer- und/oder Gruppenkonten auswählen. Des Weiteren kann festgelegt werden, welche Zugriffsart, z. B. lesender Zugriff oder Löschen von Dateien/Ordner, überwacht werden soll. Damit besteht die Möglichkeit, die zu überwachenden Aktivitäten sehr speziell festzulegen.



Überwachung des Ordners „Personalabteilung“

Stellen Sie sicher, dass sich die Administratoren in Bezug auf die Überwachungsrichtlinien nicht selbst kontrollieren. Die Zuständigkeit für die Verwaltung des Sicherheitsprotokolls sollte außerhalb der IT-Abteilung liegen (z. B. beim Datenschutzbeauftragten).

Prozessverfolgung überwachen
Empfohlene Einstellung: Keine Überwachung
Kategorie: Detaillierte Überwachung
Über die Prozessverfolgung kann überwacht werden, welcher Benutzer auf welche ausführbare Datei (z. B. exe, com oder dll) zugreift. Die Protokollierung kann nicht auf einzelne Benutzer begrenzt werden. Es entstehen deshalb bei einer Aktivierung verhältnismäßig viele Protokolleinträge. Diese Überwachungsrichtlinie sollte bei Systemstörungen eingeschaltet werden, wenn nicht genau bestimmt werden kann, welche Prozesse unter einem Benutzerkonto ablaufen.

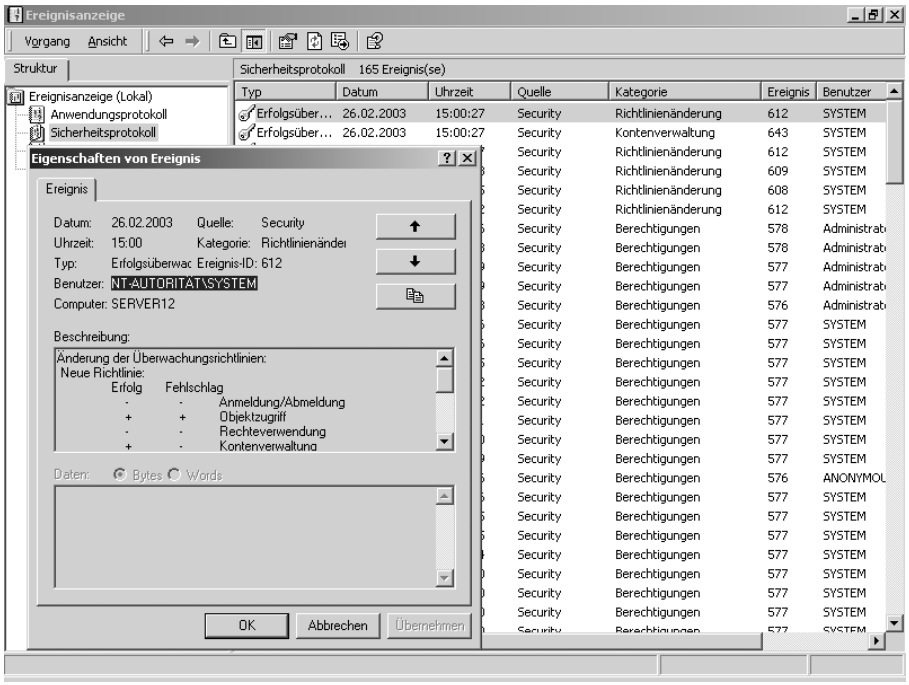
Rechteverwendung überwachen
Empfohlene Einstellung: Keine Überwachung

Kategorie: Berechtigungen
Mithilfe dieser Richtlinie kann überwacht werden, welche Systemfunktionen (siehe Kapitel 9, Tz. 9.4.2) von einem Benutzerkonto oder von dem Betriebssystem ausgeführt werden. Zu den Systemfunktionen gehören alle unter der Richtlinie ZUWEISEN VON BENUTZERRECHTEN aufgeführten Befugnisse. Da einige Systembenutzerrechte, wie z. B. das Herunterfahren des Systems oder das Anmelden an der Konsole, sehr häufig ausgeführt werden, entstehen bei der Aktivierung dieser Richtlinie sehr viele Protokolleinträge. Diese Richtlinie sollte nur im begründeten Einzelfall aktiviert werden.

Richtlinienveränderungen überwachen
Empfohlene Einstellung: Erfolgreich, Fehlgeschlagen
Kategorie: Richtlinienänderung
Es werden nur die Änderungen im Bereich der Lokalen Richtlinien (Überwachungsrichtlinien, Zuweisen von Benutzerrechten und Sicherheitsoptionen) protokolliert. Werden beispielsweise die Kontorichtlinien verändert, erscheint seltsamerweise kein Eintrag im Sicherheitsprotokoll. Die Richtlinie sollte grundsätzlich in Kombination mit jeder anderen Richtlinie aktiviert werden. Damit wird sichergestellt, dass insbesondere administrative Veränderungen im Bereich der Überwachungsrichtlinien nachvollzogen werden können.

Systemereignisse überwachen
Empfohlene Einstellung: Keine Überwachung
Kategorie: Systemereignis
Mithilfe der Systemereignisse werden z. B. Systemaktualisierungen überwacht, die während des Betriebes vorgenommen werden.

Aktivieren Sie die Überwachungsrichtlinien nur, wenn Sie damit auch Ihr Sicherheitsniveau erhöhen. Liegen beispielsweise in Ihrer Systemumgebung zahlreiche Sicherheitsmängel vor, macht es keinen Sinn, die Überwachungsrichtlinien zu aktivieren, wenn die Benutzer auf einem nicht gesicherten Weg zum Ziel kommen.



Ereignisanzeige – Sicherheitsprotokoll auf dem DC, Richtlinienveränderungen überwachen

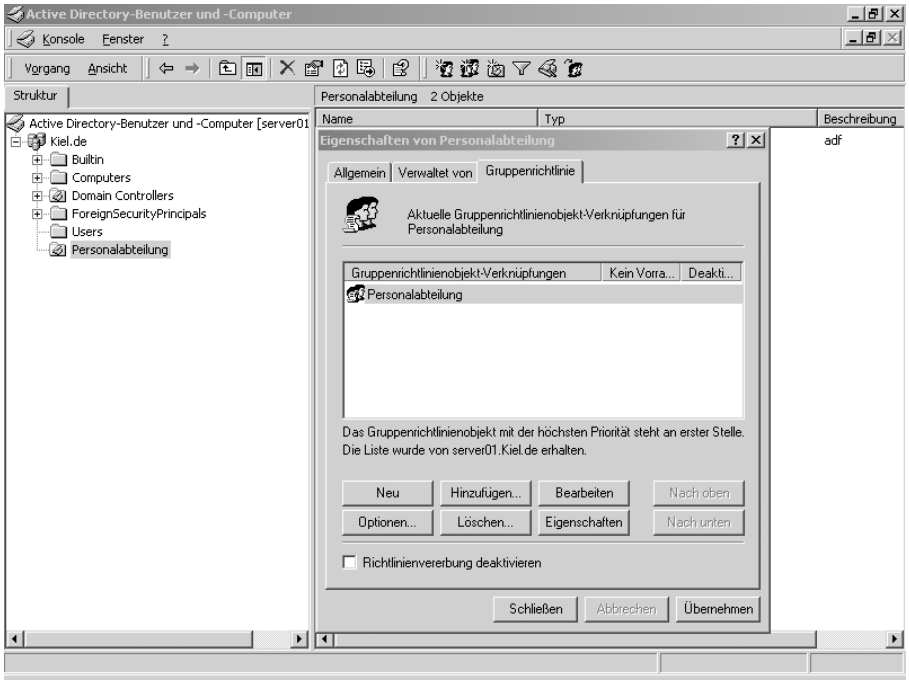
- Die vollständige Überwachung administrativer Aktivitäten wird durch die Überwachungsrichtlinien nicht unterstützt. Die Aktivierung zu vieler Überwachungsrichtlinien führt dazu, dass das Sicherheitsprotokoll aufgrund zahlreicher Einträge unübersichtlich und die Auswertung erschwert wird.

- Der Administrator wird beispielsweise über den Zugriff auf **Datensicherungsbänder** oder den Einsatz von **Hacker-Tools** Möglichkeiten finden, Sicherheitsmaßnahmen zu umgehen. So kann er z. B. mit dem Befehl `at 15:45 /interactive cmd.exe` zeitgesteuert (15.45 Uhr) die Eingabeaufforderung (cmd.exe) unter der Kennung des Systems aufrufen. Alle Aktivitäten werden dann nicht dem Benutzerkonto des Administrators sondern dem System zugeordnet.

10.8 Organisationseinheiten-Gruppenrichtlinie

In der Gruppenrichtlinie für Organisationseinheiten (OE) wirken sich die Richtlinien mit Ausnahme des Knotens SICHERHEITSEINSTELLUNGEN der Computerkonfiguration auf die Benutzer und Clients der **entsprechenden OE** aus. Es können somit unterschiedliche **Sicher-**

heitsstufen für OE implementiert werden. In einer größeren Organisation sollte eine differenzierte Zuweisung von Gruppenrichtlinien genau geplant werden.



Gruppenrichtlinie der Organisationseinheit Personalabteilung

Da die Verwaltung der Gruppenrichtlinien auf verschiedenen Ebenen **kaum** noch **nachvollziehbar** ist, ist es empfehlenswert, die Konfiguration der OE-Gruppenrichtlinien einheitlich zu gestalten. Die OE-Gruppenrichtlinie wird im ACTIVE DIRECTORY-BENUTZER UND -COMPUTER über die Eigenschaften der entsprechenden Organisationseinheit erstellt.

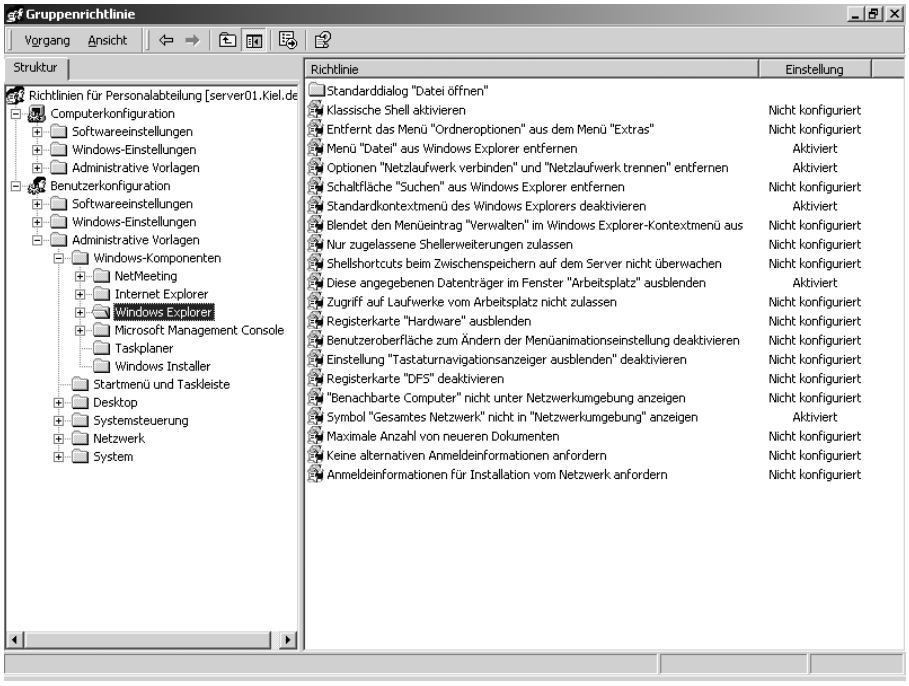
Über die Registerkarte GRUPPENRICHTLINIE kann eine neue Gruppenrichtlinie erstellt, gelöscht oder die Reihenfolge der Umsetzung bei der Verwendung mehrerer OE-Gruppenrichtlinien festgelegt werden. Des Weiteren lassen sich für das Gruppenrichtlinienobjekt auch **Berechtigungen für die Administration** vergeben. Folgende Richtlinien sollten für die Eingrenzung der Funktionen am Arbeitsplatz aktiviert werden:

Einschränkungen des Windows Explorers:
\Benutzerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Windows Explorer

Menü „Datei“ aus Windows Explorer entfernen
Empfohlene Einstellung: Aktiviert
Entfernt das Menü *Datei* aus dem Windows Explorer.

Optionen „Netzwerklaufwerk verbinden“ und „Netzwerklaufwerk trennen“ entfernen
Empfohlene Einstellung: Aktiviert
Entfernt die Menüeinträge *Netzlaufwerk verbinden* und *Netzlaufwerk trennen* von der Symbolleiste und aus den Menüs *Extras* im *Windows Explorer* und in der *Netzwerkumgebung*. Zusätzlich werden die Einträge aus den Kontextmenüs, die bei einem Rechtsklick auf die Symbole von *Windows Explorer* und *Netzwerkumgebung* angezeigt werden, entfernt. Ebenso wird die Option *Netzwerkressource hinzufügen* aus *Netzwerkumgebung* entfernt.

Standardkontextmenü des Windows Explorers deaktivieren
Empfohlene Einstellung: Aktiviert
Entfernt die Kontextmenüs vom *Desktop* und aus dem *Windows Explorer*. Kontextmenüs werden mit einem Rechtsklick auf ein Objekt angezeigt. Durch Aktivieren dieser Richtlinie werden die Menüs bei einem Rechtsklick auf den *Desktop* oder auf ein Objekt im *Windows Explorer* nicht angezeigt.



OE-Gruppenrichtlinie – Einschränkungen des Windows Explorers

Diese angegebenen Datenträger im Fenster „Arbeitsplatz“ entfernen
Empfohlene Einstellung: Aktiviert, Alle Laufwerke einschränken
Entfernt die Symbole für ausgewählte Laufwerke aus *Arbeitsplatz*, *Windows Explorer* und *Netzwerkumgebung*. Außerdem werden die Laufwerkbuchstaben, die die ausgewählten Laufwerke darstellen, im Standarddialog *Öffnen* nicht angezeigt.

Symbol „Gesamtes Netzwerk“ nicht in „Netzwerkumgebung“ anzeigen
Empfohlene Einstellung: Aktiviert
Entfernt alle Computer, die nicht zu der Arbeitsgruppe oder lokalen Domäne des Benutzers gehören, aus den Listen der Netzwerkressourcen im *Windows Explorer* und in der *Netzwerkumgebung*.

Startmenü und Taskleiste
\Benutzerkonfiguration\Administrative Vorlagen\Startmenü und Taskleiste

Verknüpfungen für Windows Update deaktivieren und entfernen
Empfohlene Einstellung: Aktiviert
Durch Aktivieren dieser Richtlinie können Benutzer nicht auf die Windows Update-Website (http://windowsupdate.microsoft.com) zugreifen. Zusätzlich wird der Hyperlink *Windows Update* aus dem *Startmenü* und aus dem Menü *Extras* im *Internet Explorer* entfernt.

Standardpogrammgruppen aus dem Startmenü entfernen
Empfohlene Einstellung: Aktiviert
Standardmäßig enthält das Menü *Programme* Objekte aus dem Profil *All Users* und Objekte aus dem Profil des Benutzers. Durch Aktivieren dieser Richtlinie, werden nur die Objekte aus dem Profil des Benutzers im Menü *Programme* angezeigt.

Programme im Menü „Einstellungen“ deaktivieren
Empfohlene Einstellung: Aktiviert
Durch diese Richtlinie werden die Ordner *Systemsteuerung*, *Drucker* und *Netzwerk- und DFÜ-Verbindungen* aus dem Menü *Einstellungen* im *Startmenü*, aus *Arbeitsplatz* und *Windows Explorer* entfernt. Zusätzlich können die Programme (wie z. B. Control.exe), die mit diesen Ordnern assoziiert sind, nicht ausgeführt werden.

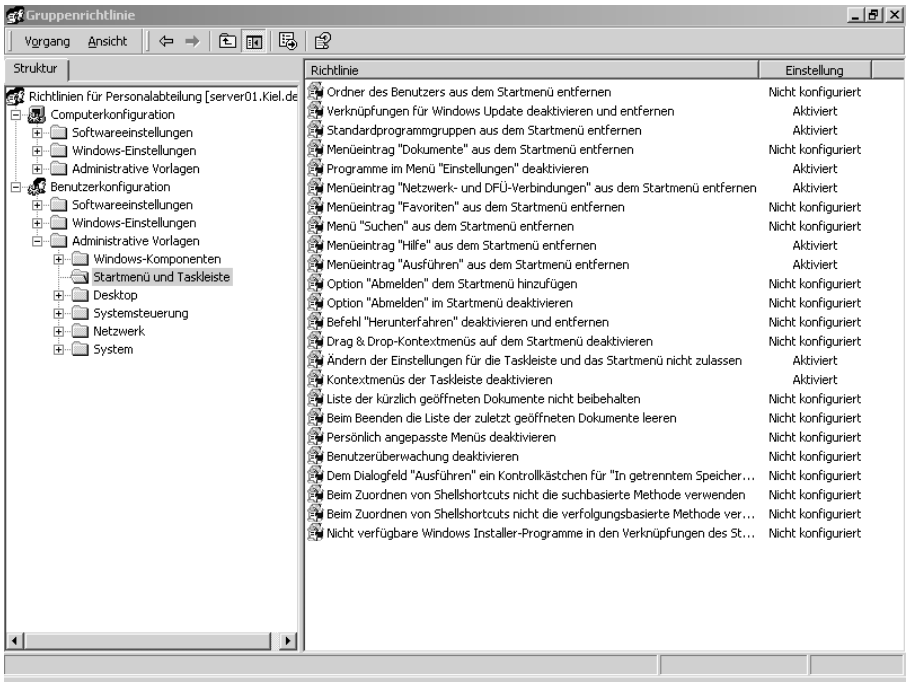
Menüeintrag „Netzwerk- und DFÜ-Verbindungen“ aus dem Startmenü entfernen
Empfohlene Einstellung: Aktiviert
Diese Richtlinie verhindert, dass der Ordner *Netzwerk- und DFÜ-Verbindungen* geöffnet wird. zusätzlich wird der Eintrag *Netzwerk- und DFÜ-Verbindungen* aus dem Menü *Einstellungen* im Startmenü entfernt.

Menüeintrag „Hilfe“ aus dem Startmenü entfernen
Empfohlene Einstellung: Aktiviert
Der Menüeintrag *Hilfe* wird aus dem Startmenü entfernt.

Menüeintrag „Ausführen“ aus dem Startmenü entfernen
Empfohlene Einstellung: Aktiviert
Der Menüeintrag *Ausführen* und der Befehl *Neuer Task (Ausführen)...* im Task-Manager wird aus dem Startmenü entfernt. Zusätzlich können Benutzer mit erweiterten Tastaturen das Dialogfeld *Ausführen* nicht mehr mit der Anwendungstaste (die Taste mit dem Windows-Logo) +R anzeigen.

Ändern der Einstellungen für die Taskleiste und das Startmenü nicht zulassen
Empfohlene Einstellung: Aktiviert
Der Menüeintrag *Taskleiste und Startmenü* aus dem Menü *Einstellungen* im Startmenü wird ausgeblendet. Diese Richtlinie verhindert, dass Benutzer das Dialogfeld *Eigenschaften von Taskleiste und Startmenü* öffnen.

Kontextmenü der Taskleiste deaktivieren
Empfohlene Einstellung: Aktiviert
Die Menüs, die mit einem Rechtsklick auf die Taskleiste angezeigt werden, und die Objekte auf der Taskleiste, (z. B. die Schaltfläche *Start*, die Uhr und die Schaltflächen der Taskleiste) werden ausgeblendet.

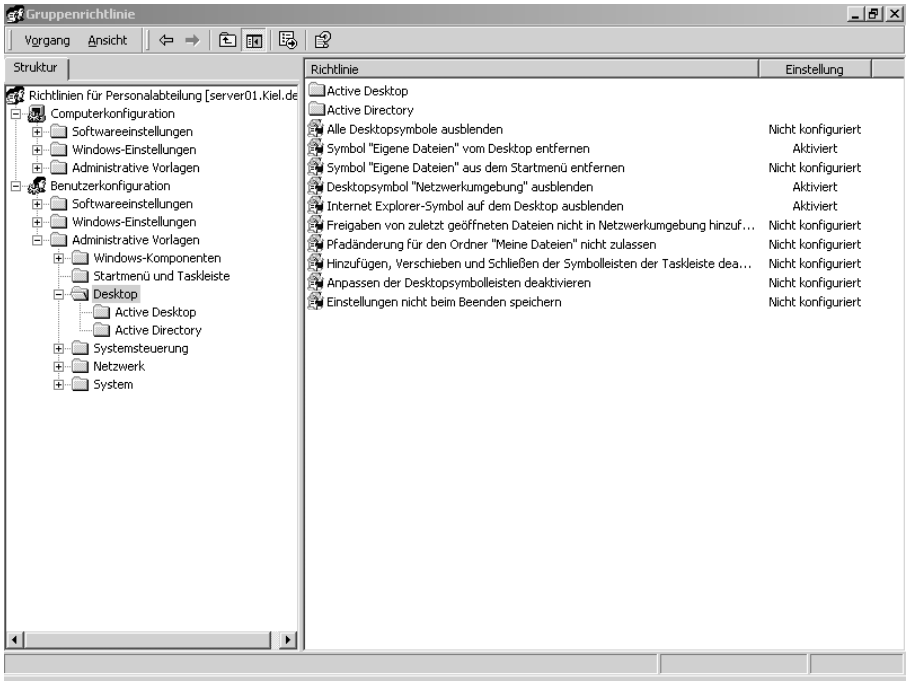


OE-Gruppenrichtlinie – Einschränkungen des Startmenüs und der Taskleiste

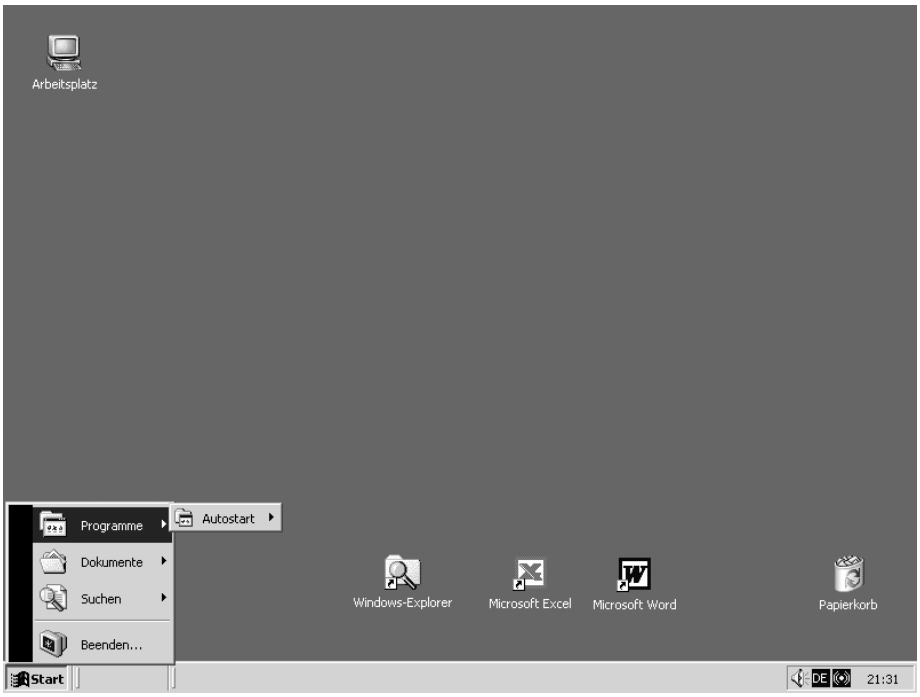
Desktop

\Benutzerkonfiguration\Administrative Vorlagen\Desktop

Symbol „Eigene Dateien“ vom Desktop entfernen
Empfohlene Einstellung: Aktiviert
Durch diese Richtlinie wird das Symbol *Eigene Dateien* vom Desktop, aus dem *Windows Explorer*, aus Programmen, die das Windows Explorer-Fenster verwenden und aus dem Standarddialog *Öffnen* entfernt.



OE-Gruppenrichtlinie – Einschränkungen der Desktopoberfläche



Desktopoberfläche durch Einschränkungen über OE-Gruppenrichtlinien

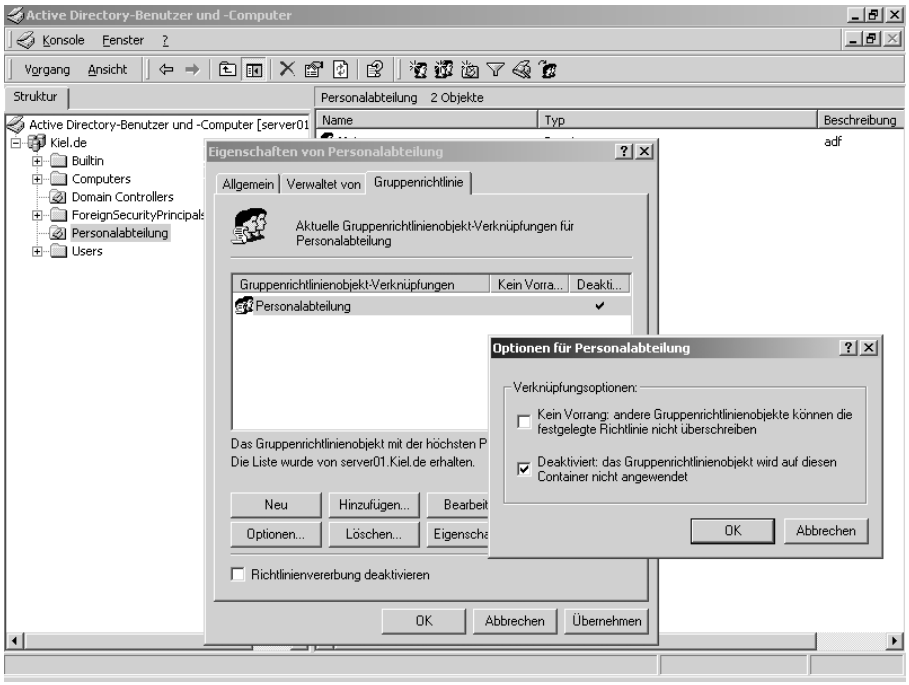
Desktopsymbol „Netzwerkumgebung“ ausblenden
Empfohlene Einstellung: Aktiviert
Das Symbol *Netzwerkumgebung* wird vom Desktop entfernt.

Internet Explorer-Symbol auf dem Desktop ausblenden
Empfohlene Einstellung: Aktiviert
Das Symbol *Internet Explorer* wird vom Desktop und von der Schnellstartleiste auf der Taskleiste entfernt.

10.9 Gruppenrichtlinien einschränken

Die Umsetzung von Gruppenrichtlinien kann mit folgenden **Funktionen** unterbunden bzw. eingeschränkt werden.

- Die ausgewählte Gruppenrichtlinie wird über die Schaltfläche OPTIONEN mit dem Schalter DEAKTIVIERT: DAS GRUPPENRICHTLINIENOBJEKT WIRD AUF DIESEN CONTAINER NICHT ANGEWENDET deaktiviert. Alle Einschränkungen werden **automatisch** aufgehoben, so dass sie sich auf die Objekte der Organisationseinheit (OE) nicht mehr auswirken.



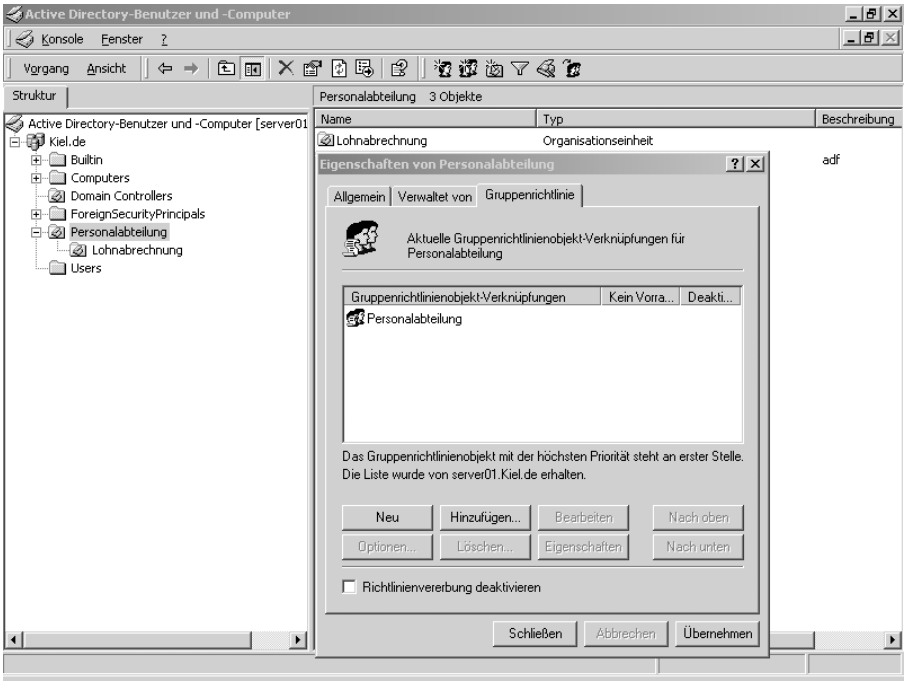
Organisationseinheiten-Gruppenrichtlinie deaktivieren

- Des Weiteren kann unter dieser Option mit dem Schalter KEIN VORRANG: ANDERE GRUPPENRICHTLINIENOBJEKTE KÖNNEN DIE FESTGELEGTE RICHTLINIE NICHT ÜBERSCHREIBEN die Umsetzung und somit das Überschreiben durch **nachfolgende Gruppenrichtlinien** verhindert werden. Wird diese Option z. B. in der Gruppenrichtlinie DEFAULT DOMAIN

POLICY aktiviert, können Gruppenrichtlinien, die auf der Ebene der Organisationseinheiten eingerichtet sind, die DEFAULT DOMAIN POLICY nicht überschreiben.

- Der Schalter RICHTLINIENVERERBUNG DEAKTIVIEREN bewirkt, dass eine Gruppenrichtlinie einer Ebene sich nicht auf eine untergeordnete Ebene auswirkt. Wird z. B. in der OE Personalabteilung eine untergeordnete OE Lohnabrechnung angelegt, dann wird zunächst standardmäßig die Gruppenrichtlinie der OE Personalabteilung automatisch auch auf die OE Lohnabrechnung angewendet. Wird der Schalter RICHTLINIENVERERBUNG DEAKTIVIEREN unter der OE Lohnabrechnung aktiviert, wirkt sich die Gruppenrichtlinie der OE Personalabteilung nicht mehr auf die OE Lohnabrechnung aus.

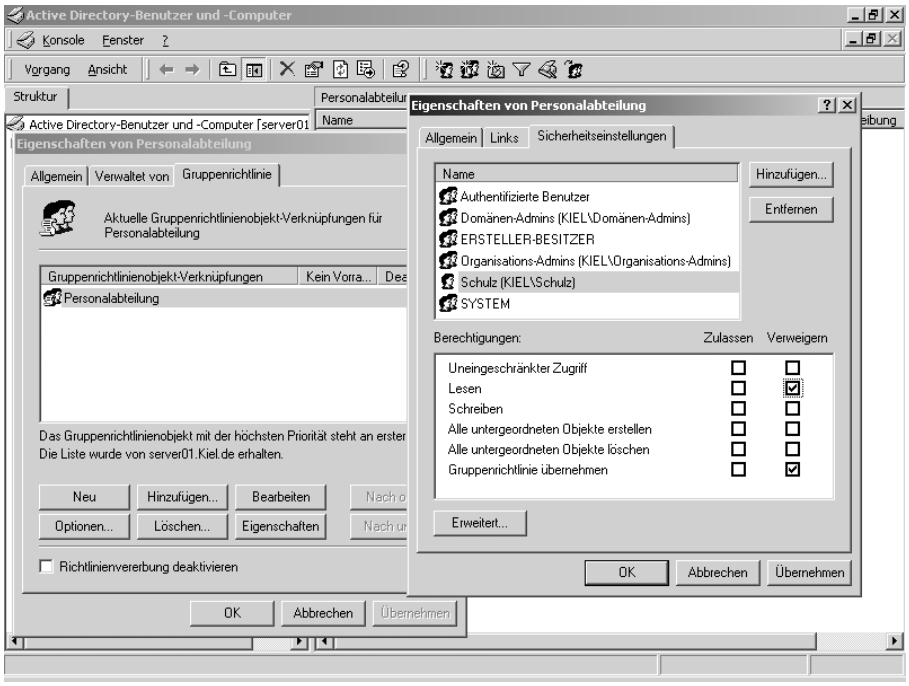
Der Knoten Sicherheitseinstellungen der Computerkonfiguration der DEFAULT DOMAIN POLICY wird von einer Deaktivierung der Richtlinienvererbung ausgeschlossen.



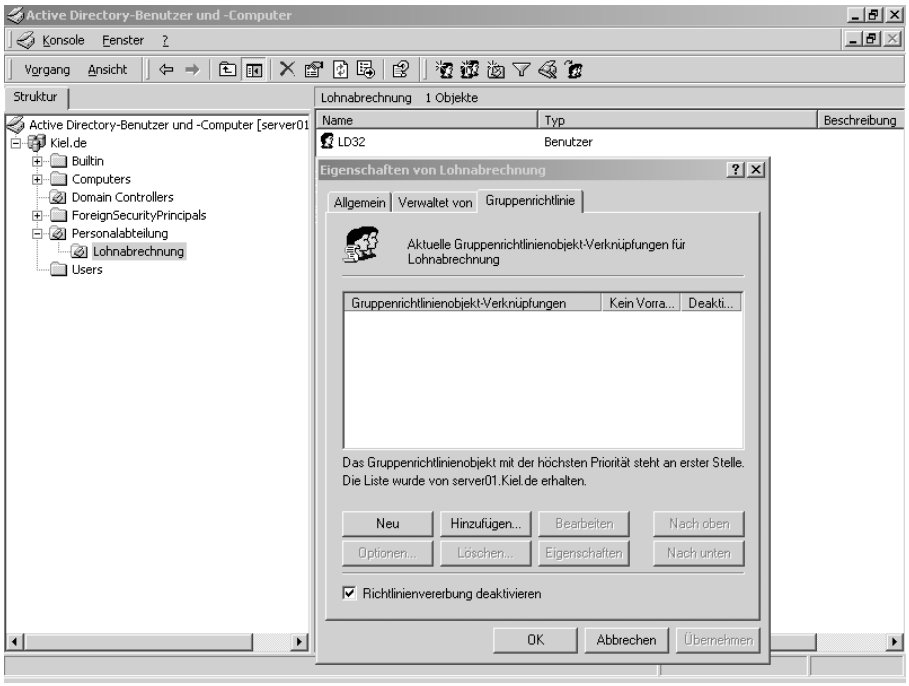
Gruppenrichtlinie der OE Personalabteilung

- Standardmäßig wirken sich die Gruppenrichtlinien auf alle Benutzer oder Computer eines Standortes, einer Domäne oder auf die Organisationseinheit aus. Der Gruppe *Authentifizierte Benutzer* werden die Rechte *Lesen* und *Gruppenrichtlinie übernehmen* zugewiesen, so dass auf den Benutzer bei der Anmeldung am Client automatisch die Gruppenrichtlinie angewendet wird. Anhand der Berechtigungen der Benutzerkonten auf ein Gruppenrichtlinienobjekt kann jedoch die **Wirkung bzw. Umsetzung** der Gruppenrichtlinie verweigert werden.

In der u. a. Abbildung ist eine Gruppenrichtlinie der OE PERSONALABTEILUNG zugewiesen worden. Über die Gruppe *Authentifizierte Benutzer* unterliegen alle Benutzerkonten der OE den Einschränkungen der Gruppenrichtlinie.



OE Lohnabrechnung – Gruppenrichtlinienanwendung der OE Personalabteilung deaktivieren



Übernahme der Gruppenrichtlinie einem Benutzerkonto verweigern

Mit der Aufnahme des Benutzerkontos SCHULZ wurde jedoch die Übernahme der Gruppenrichtlinie durch die Zuweisung der Berechtigung GRUPPENRICHTLINIE ÜBERNEHMEN VERWEI-

GERN unterbunden. Wenn sich also der Benutzer SCHULZ am Client anmeldet, unterliegt er nicht den Einschränkungen der Gruppenrichtlinie PERSONALABTEILUNG.

Der Einsatz mehrerer Filter kann schnell zu einer unübersichtlichen Berechtigungsvergabe führen. Verwenden Sie deshalb einen Gruppenrichtlinienfilter nur in Ausnahmesituationen.

10.10 Richtlinienergebnissatz

Der RICHTLINIENERGEBNISSATZ (Resultant Set of Policy = RsoP.msc) ist eine neue Snap-In-Ergänzung zu den Gruppenrichtlinien und steht erst unter Windows Server 2003 und XP zur Verfügung. Bei diesem Snap-In handelt es sich um ein **Abfragemodul**, das die vorhandenen Richtlinien auswertet und in der gewohnten Gruppenrichtlinienstruktur anzeigt. Es kann dann unabhängig von der Umsetzung einer Richtlinie nachvollzogen werden, welche Gruppenrichtlinie welche Einschränkungen enthält. Probleme in Bezug auf eine fehlerhafte Umsetzung von Richtlinien lassen sich so schneller lösen.

10.11 Gruppenrichtlinien-Tool

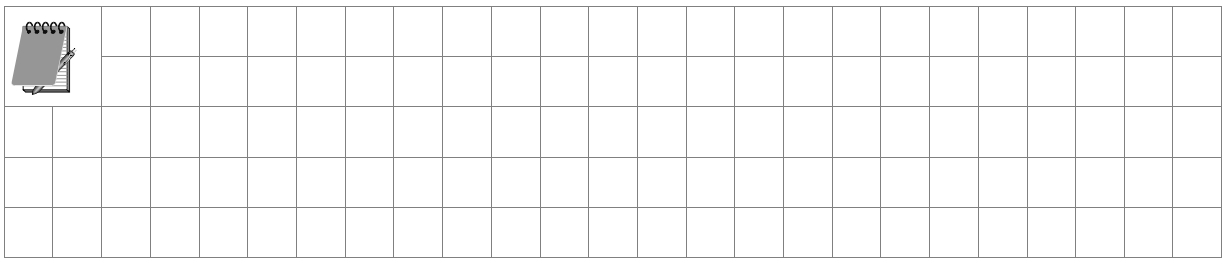
Das Windows 2000 Resource-Kit enthält ein nützliches Tool für den Test von Gruppenrichtlinien. Das Tool GPRESULT ist ein Befehlszeilenprogramm, das folgende Informationen zu Gruppenrichtlinien bereit stellt:

- Letzte Anwendung einer Gruppenrichtlinie,
- vollständige Liste der angewendeten Richtlinien,
- umgesetzte Registrierungseinstellungen,
- umgeleitete Ordner,
- Softwareverwaltungsinformationen,
- Informationen zu Datenträgerkontingenten und
- IP-Sicherheitseinstellungen.

Die Informationen der einzelnen Bereiche können teilweise über die Angabe eines Parameters ausgewertet werden. Bei dem Betriebssystem Windows Server 2003 gehört das Tool bereits zur „Standardausstattung“.

10.12 Sicherheitscheck

- *Vor der Konfiguration der Gruppenrichtlinien sollten Sie sich genau über die **Funktionsweise** informieren.*
- *Richten Sie eine **Testorganisationseinheit** und ein **Test-Benutzerkonto** für die Umsetzung der Gruppenrichtlinien ein.*
- *Planen Sie, welche Einschränkungen in Ihrer Systemumgebung erforderlich sind. Orientieren Sie sich dabei an dem in Ihrer Organisation vorhandenen **Sicherheitskonzept**.*
- *Berücksichtigen Sie bei der Administration der Gruppenrichtlinien die **Vererbungsreihenfolge**.*
- *Setzen Sie während der Durchführung der Tests das **Zeitintervall** für die Aktualisierung der Gruppenrichtlinien auf 0 Minuten.*
- *Auf der Ebene der **Domänen-Gruppenrichtlinien** sollten Einschränkungen vorgenommen werden, die uneingeschränkt für alle Benutzer und Computer gelten. Dazu zählen insbesondere die Kontorichtlinien.*
- *Sofern administrative Aktivitäten **überwacht** werden sollen, aktivieren Sie die Überwachungsrichtlinien in der Gruppenrichtlinie für Domänencontroller.*
- *Führen Sie in der Gruppenrichtlinie für **Organisationseinheiten** Einschränkungen unter der BENUTZERKONFIGURATION durch, so dass die Funktionen auf dem Desktop eines Benutzers auf das erforderliche Maß reduziert werden.*
- *Setzen Sie ggf. für die **Kontrolle** der Konfigurationseinstellungen das Tool GPRESULT aus dem Windows 2000 Resource-Kit ein. Sofern Windows Server2003 bzw. XP eingesetzt wird, sollte zusätzlich der RICHTLINIENERGEBNISSATZ berücksichtigt werden.*



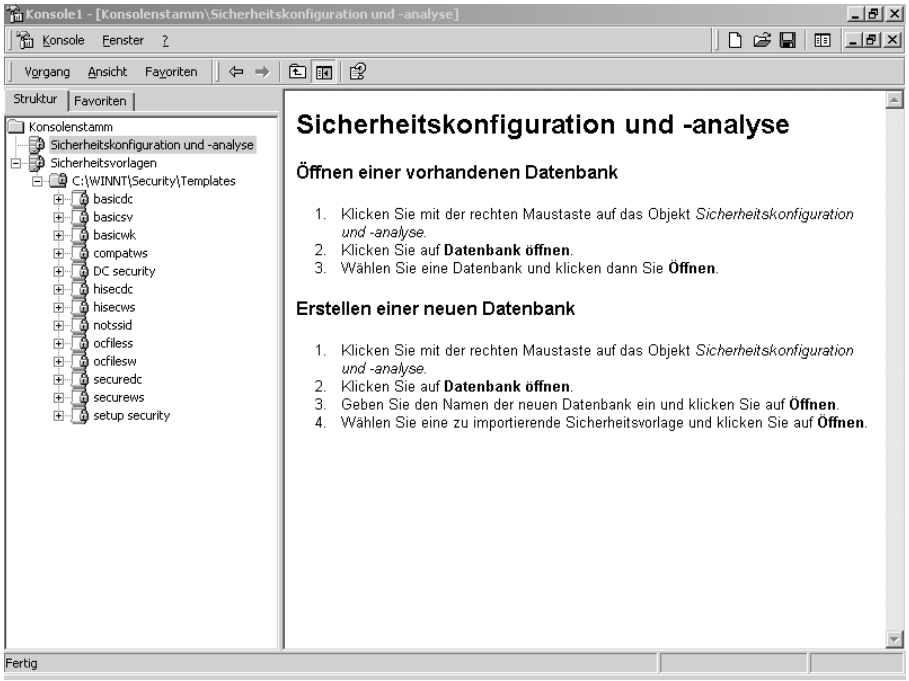
11 Sicherheitsanalyse und Sicherheits-Tools

In diesem Kapitel erfahren Sie,

- mit welchem Verwaltungsprogramm die Sicherheitseinstellungen analysiert werden können,
- was bei einer Sicherheitsanalyse und einer Sicherheitskonfiguration zu beachten ist,
- warum es wichtig ist, die Sicherheitseinstellungen nachvollziehbar darzustellen,
- wie Disketten- und CD-ROM-Laufwerke gesperrt werden können,
- welche Systemdateien auf der Festplatte in die Defragmentierung einbezogen werden sollten und
- dass gelöschte Dateien über den Einsatz von Tools wiederherstellbar sind.

11.1 Sicherheitskonfiguration und -analyse

Mit dem Snap-In SICHERHEITSKONFIGURATION UND -ANALYSE wird die Sicherheit des lokalen Computers analysiert und konfiguriert.



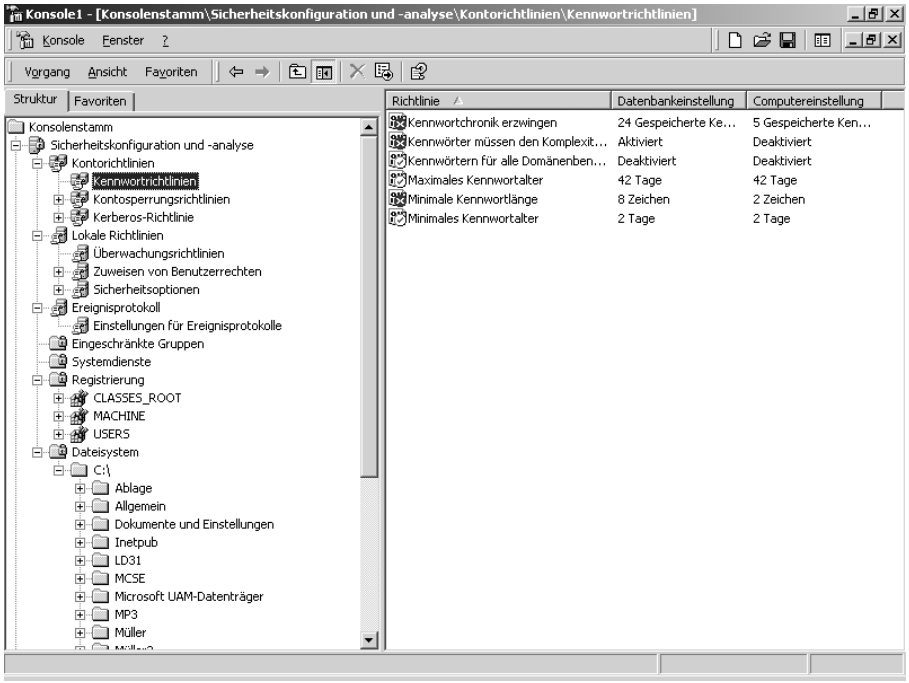
Snap-In Sicherheitskonfiguration und -analyse, Sicherheitsvorlagen

Der aktuelle Status der Systemsicherheit wird mit einer Sicherheitsvorlage verglichen. Die Sicherheitsvorlagen werden für die Analyse über das Snap-In SICHERHEITSVORLAGEN zunächst in eine Datenbank importiert.

Die Sicherheitskonfigurationsanalyse bezieht sich auf **Systemeinstellungen** im Bereich

- der Kontorichtlinien,
- der Lokalen Richtlinien,
- der Einstellungen für das Ereignisprotokoll,
- der Systemdienste,
- der Registrierung und
- der Berechtigungsvergabe für Ordner und Dateien (Dateisystem).

Die vorgegebenen Einstellungen aus der importierten Sicherheitsvorlage werden unmittelbar den Computereinstellungen gegenübergestellt, sodass ein Vergleich zwischen Soll und Ist nachvollziehbar wird. Abweichungen werden über ein **rotes Kreuz** signalisiert.



Auswertungsinformationen durch die Durchführung der Sicherheitsanalyse

Folgende Sicherheitsvorlagen stehen für die Analyse und Konfiguration zur Verfügung:

- Standardarbeitsstation (**basicwk.inf**),
- Standardserver (**basicsv.inf**),
- Standarddomänencontroller (**basicdc.inf**),
- kompatible Arbeitsstation oder Server (**compatws.inf**),
- Domänencontroller, aktualisierte Standardsicherheitseinstellungen (**DC security.inf**),
- sichere Arbeitsstation oder Server (**securews.inf**),
- sehr sichere Arbeitsstation oder Server (**hisecws.inf**),
- Windows 2000-Terminalserver (**notssid.inf**),
- sicherer Domänencontroller (**securedc.inf**),
- sehr sicherer Domänencontroller (**hisecdc.inf**),
- sicherer Dateiserver (**ocfiless.inf**),
- sichere Arbeitsstationen (**ocfilesw.inf**),
- Windows 2000-Standardsicherheitskonfiguration (**setup security.inf**).

Die Vorlagen werden im Ordner <Stammverzeichnis:\winnt\security\templates> verwaltet. Sie sind darauf ausgelegt, vier häufig vorkommende Sicherheitsanforderungen abzudecken:

- **Basis (basicwk.inf, basicsv.inf, basicdc.inf)**

  Mit den Vorlagen für die Basiskonfiguration kann die Anwendung einer anderen Sicherheitskonfiguration aufgehoben werden. Die Basiskonfigurationen wenden die Standardsicherheitseinstellungen von Windows 2000 auf alle Sicherheitsbereiche an. Eine Ausnahme bilden die Sicherheitsbereiche, die sich auf Benutzerrechte beziehen. Diese werden nicht in den Basisvorlagen geändert, da Benutzerrechte üblicherweise durch Setupprogramme von Anwendungen angepasst werden, um eine erfolgreiche Verwendung der Anwendung zu ermöglichen. Solche Anpassungen sollen nicht durch die Basiskonfigurationsdateien rückgängig gemacht werden.

- **Kompatibel (compatws.inf)**

  In der Standardeinstellung sind die Sicherheitsfunktionen von Windows 2000 so konfiguriert, dass Mitglieder der lokalen Benutzergruppe über strenge Sicherheitseinstellungen verfügen, während die Sicherheitseinstellungen für die Mitglieder der lokalen Hauptbenutzergruppe mit den Windows NT 4.0-Benutzerzuweisungen kompatibel sind. Die kompatible Vorlage ermöglicht ein erfolgreiches Ausführen der meisten Anwendungen unter einem Benutzerkonto.

- **Sicher (securews.inf, securedc.inf)**

  Die sicheren Vorlagen implementieren die empfohlenen Sicherheitseinstellungen für alle Sicherheitsbereiche mit Ausnahme von Dateien, Ordnern und Registrierungsschlüsseln. Diese werden nicht geändert, da Dateisystem- und Registrierungsberechtigungen standardmäßig sicher konfiguriert werden.

- **Sehr sicher (hisecws.inf, hisecdc.inf)**

  Die sehr sicheren Vorlagen definieren zusätzlich Einstellungen für die Netzkonfiguration unter Windows 2000. Die Sicherheitsbereiche bieten maximalen Schutz für den Netzwerkverkehr sowie für Netzwerkprotokolle für Computer, auf denen Windows 2000 ausgeführt wird.

Die Sicherheitsvorlagen NOTSSID.INF, OCFILESS.INF, OCFILESW.INF und SETUP SECURITY.INF fügen Sicherheitseinstellungen für optionale Komponenten wie Terminaldienste oder Zertifikatsdienste hinzu.

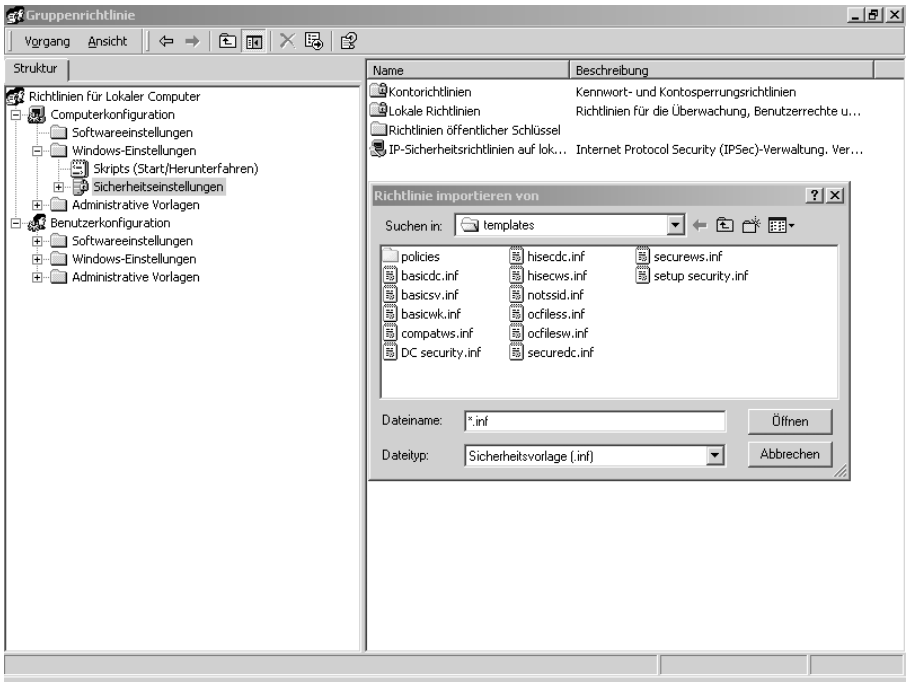
Sicherheitskonfigurationsanalyse durchführen!

1. *Klicken Sie im Snap-In SICHERHEITSKONFIGURATION UND -ANALYSE mit der rechten Maustaste auf SICHERHEITSKONFIGURATION UND -ANALYSE.*
2. *Wenn noch keine Datenbank festgelegt wurde, klicken Sie auf DATENBANK ÖFFNEN, um eine Datenbank zu bestimmen.*
3. *Klicken Sie auf VORLAGE IMPORTIEREN.*
4. *Wählen Sie eine Sicherheitsvorlagendatei aus und klicken Sie auf ÖFFNEN.*
5. *Klicken Sie mit der rechten Maustaste auf SICHERHEITSKONFIGURATION UND -ANALYSE und wählen Sie danach COMPUTER JETZT ANALYSIEREN.*

Neben der Sicherheitskonfigurationsanalyse können über die Option SYSTEM JETZT KONFIGURIEREN die Einstellungen einer Vorlage auf das System übertragen werden. Mit dieser Option muss sehr vorsichtig umgegangen werden. Die Einstellungen sollten nur dann übernommen werden, wenn nachvollzogen werden kann, welche Änderungen am System durchgeführt werden. Das ist nur dann gewährleistet, wenn **alle Einstellungen** einer Sicherheitsvorlage bekannt sind und diese ggf. auf die sicherheitstechnischen Erfordernisse angepasst wurden.

Vorlagen können auch einer Gruppenrichtlinie zugeordnet werden. Durch das Importieren einer Sicherheitsvorlage in ein Gruppenrichtlinienobjekt wird gewährleistet, dass sämtliche Konten, denen das Gruppenrichtlinienobjekt zugeordnet ist, automatisch die Sicherheitseinstellungen der Vorlage erhalten, wenn die Gruppenrichtlinieneinstellungen aktualisiert werden.

Sie können Sicherheitsvorlagen unter einem anderen Namen speichern und die Vorlagen dann in die Datenbank importieren. Passen Sie ggf. eine Sicherheitsvorlage Ihren Sicherheitsanforderungen an, sodass Sie sie für die Überprüfung bzw. zum Abgleichen der tatsächlichen Einstellungen auf dem Produktionssystem verwenden können.



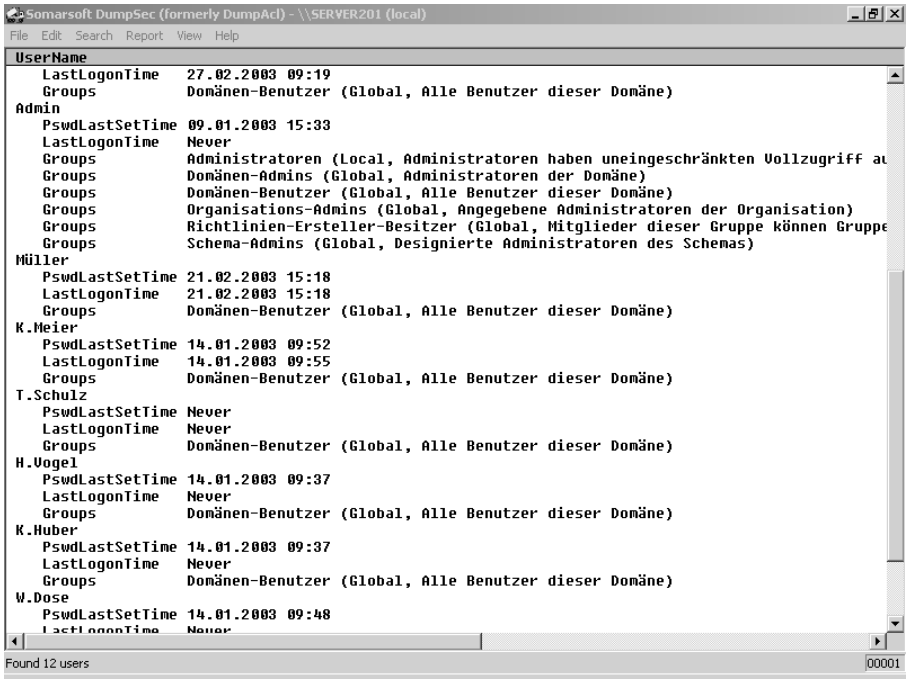
Sicherheitsvorlage in Gruppenrichtlinie importieren

- Beachten Sie, dass über die Option SYSTEM JETZT KONFIGURIEREN die Einstellungen einer Sicherheitsvorlage **ohne Sicherheitsabfrage** auf das System übertragen werden. Das Gleiche gilt für das Importieren einer Sicherheitsvorlage in eine Gruppenrichtlinie.

- Unüberlegte Aktionen oder falsche Einstellungen können dazu führen, dass das Produktionssystem nicht mehr störungsfrei läuft. Es wird deshalb empfohlen, zunächst auf einem Testsystem die Auswirkungen einer auf das System übertragenen Sicherheitsvorlage zu prüfen.

11.2 DumpSec

- Die sicherheitstechnischen Einstellungen können unter Windows 2000 nur mit erhöhtem administrativem Aufwand nachvollziehbar dargestellt werden. Es gibt keine Ausdruckfunktionen, die die Systemeinstellungen überschaubar darstellen.

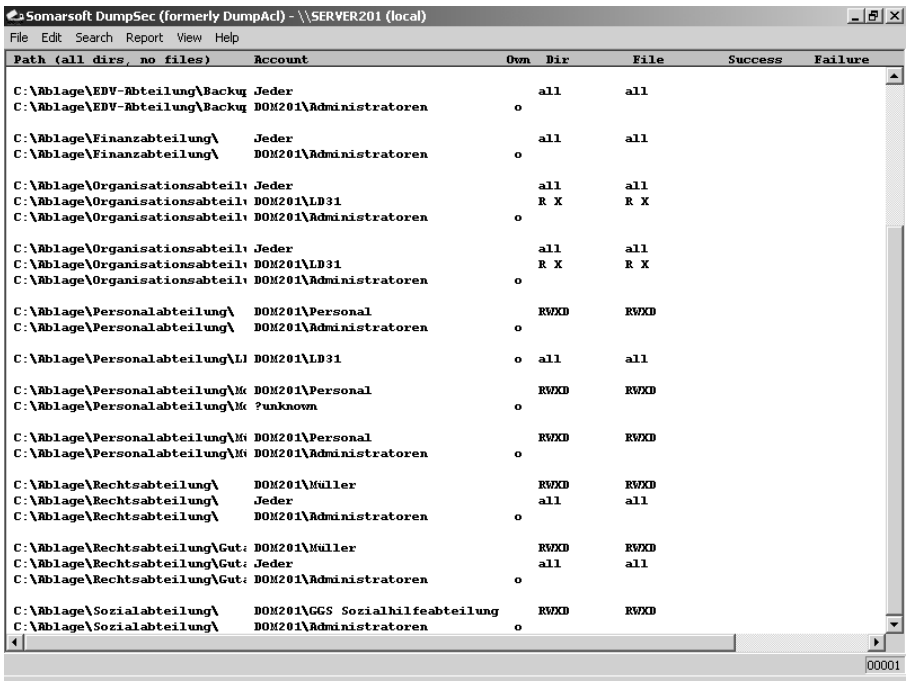


DumpSec – Benutzer- und Gruppenkontenauswertung

Mithilfe des Tools *DumpSec* von der Firma „Somarsoft“ können jedoch zusammenfassende **Reports** über Konfigurationseinstellungen aus den nachfolgenden Bereichen erstellt werden:

- Benutzer- und Gruppenkontenverwaltung,
- Freigabe- und NTFS-Berechtigungen,
- Benutzer- bzw. Systemrechte,
- Berechtigungen der Registryeinträge,
- Diensteverwaltung und

Konto- und Überwachungsrichtlinien.Es lassen sich zu den oben angegebenen Bereichen Informationen **differenziert** nach verschiedenen Kriterien am Bildschirm darstellen. Durch die Eingabe oder Auswahl der entsprechenden Auswertungskriterien werden dem Administrator die Systeminformationen, die er benötigt, in Listenform angezeigt. Sie können in einer Datei abgespeichert oder unmittelbar ausgedruckt werden. Somit ist eine Kontrolle und Überwachung der administrativen Konfigurationseinstellungen zumindest in den oben angegebenen Bereichen ohne großen Dokumentationsaufwand möglich.



DumpSec – NTFS-Berechtigungsauswertung

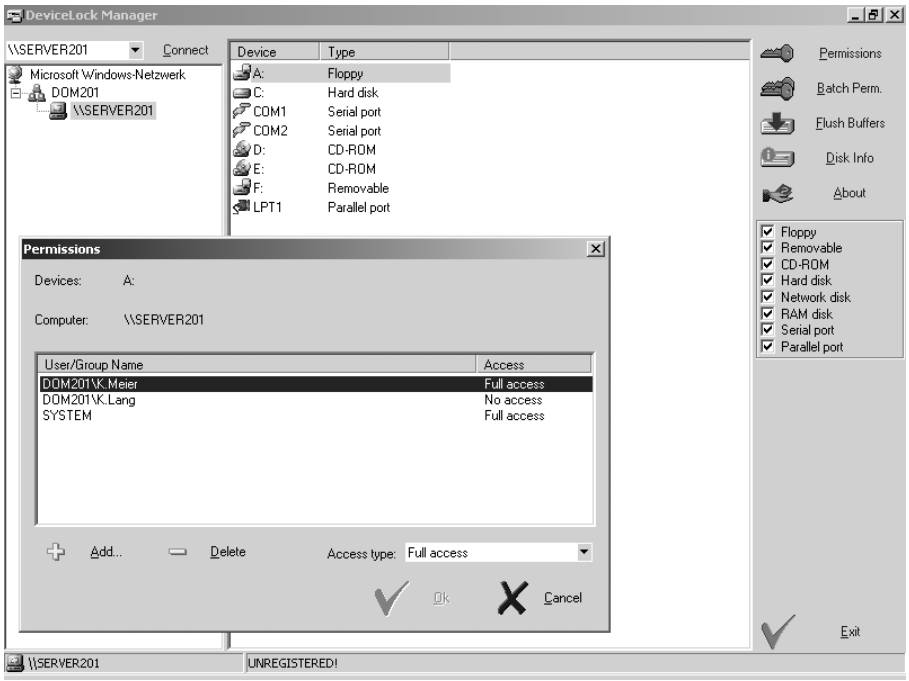
Eine in Bezug auf die Nachvollziehbarkeit der durchgeführten Einstellungen große Arbeitserleichterung liegt in der Kontrolle der den Benutzer- und Gruppenkonten zugewiesenen Freigabe- und NTFS-Berechtigungen. Die auf dem Datenträger eingerichteten Ordner lassen sich

bezüglich der zugewiesenen Berechtigungen individuell auswerten. Der Aufruf der Registerkarte SICHERHEITSEINSTELLUNGEN für jeden zu überprüfenden Ordner ist nicht mehr nötig.

DUMPSEC kann von der Webseite www.systemTools.com (siehe Kapitel 13) als Freeware heruntergeladen und sofort eingesetzt werden.

11.3 DeviceLock

Auch unter Windows 2000 lassen sich die Disketten- und CD-ROM-Laufwerke der Arbeitsplatz-PC nicht benutzerbezogen zuordnen. Um diese Schwachstelle in den Griff zu bekommen, werden die Laufwerke häufig im BIOS ausgeschaltet. Das hat jedoch den Nachteil, dass von dieser Maßnahme auch die Administration betroffen ist. Ferner werden auf einigen Arbeitsplätzen die Laufwerke für dienstliche Aufgaben benötigt, sodass auf diesen PC dann z. B. Diskettenschlösser eingesetzt werden.



DeviceLock-Manager

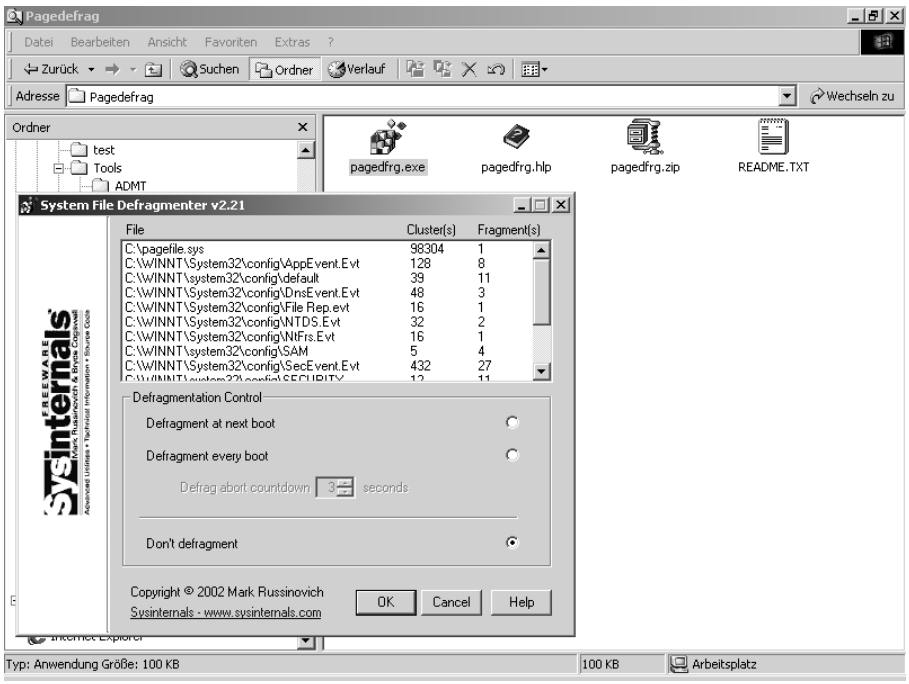
Mit dem Security-Tool *DeviceLock* können dagegen die Laufwerke bequem benutzerbezogen verwaltet werden. Die Installation des Tools ist über das Netzwerk durchführbar. Zentral kann für jeden Arbeitsplatz festgelegt werden, welches Benutzerkonto z. B. ein Disketten- und CD-ROM-Laufwerk nutzen darf. Darüber hinaus werden in *DeviceLock* auch die Schnittstellen des Computers, wie z. B. die seriellen und parallelen Ports, zusätzliche Festplatten und Spei-

chererweiterungen, wie z. B. USB-Sticks, mit einbezogen. Eine mühsame Administration der Arbeitsplätze vor Ort ist nicht notwendig.

Auf der Webseite www.protect-me.com (siehe Kapitel 13) wird der Funktionsumfang des Tools (V5.02) beschrieben. Es kann heruntergeladen und für 30 Tage in der Vollversion getestet werden. Eine Einzelplatzlizenz liegt bei 35 Dollar, während eine Lizenz für das gesamte Netzwerk 1500 Dollar kostet. Nach Ablauf der „Testtage“ kann das Tool nur noch genutzt werden, wenn es registriert wird.

11.4 Pagedefrag

Windows 2000 hat im laufenden Betrieb Systemdateien geöffnet, die sich mit den mitgelieferten Defragmentierungs-Tools nicht defragmentieren lassen. Zu den Systemdateien gehören die Datei *pagefile.sys* sowie die im Ordner <Stammverzeichnis:\winnt\system32\config\> verwalteten Registrydateien.



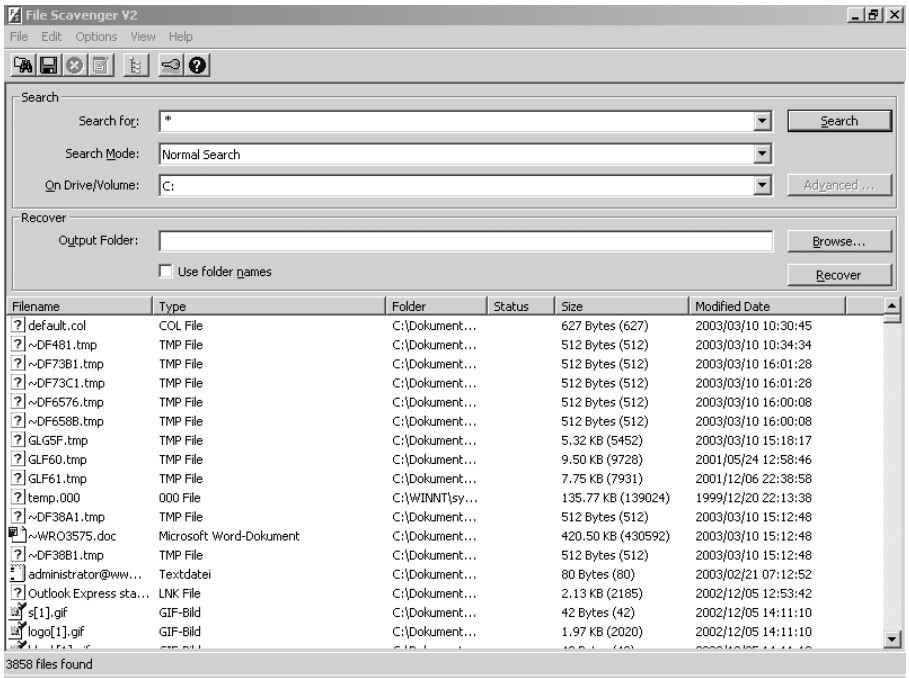
Defragmentierungstool

Insbesondere die Datei PAGEFILE.SYS wird aufgrund ihrer Größe im Laufe der Zeit in vielen Fragmenten auf der Festplatte gespeichert. Das führt häufig zu erheblichen Performancebeeinträchtigungen.

Wie in Kapitel 9 beschrieben, sollte für die Systemdateien eine ausreichend konstante Speichergröße vorgegeben werden. Dadurch wird verhindert, dass die Systemdateien im Laufe des Betriebes an Kapazität zunehmen. Wenn zusätzlich ein Defragmentierungstool, z. B. pagedefrag (www.sysinternals.com), eingesetzt wird, das die Systemdateien während der Bootphase defragmentiert, kann die Verfügbarkeit des Betriebssystems erheblich verbessert werden.

11.5 File Scavenger

Löscht ein Benutzer eine Datei von der Festplatte, wird diese zunächst in den Papierkorb verlagert. Erst wenn dieser geleert wird, wird die Datei unwiederbringlich von der Festplatte gelöscht. Mit einfachen Mitteln lassen sich jedoch selbst vor langer Zeit gelöschte Dateien wiederherstellen. Es gibt Tools, die die Festplatte nach gelöschten Dateien untersuchen und diese in aller Regel vollständig rekonstruieren. Aufgrund der großen Festplattenkapazitäten werden gelöschte Dateien selten physikalisch überschrieben. Das passiert erst dann, wenn die Festplattenkapazität zur Neige geht oder wenn die nicht gelöschten Dateien auf der Festplatte durch eine Defragmentierung in Speicherbereiche gelöschter Dateien gespeichert werden.



File Scavenger

Es besteht also ein erhebliches **Datensicherheitsproblem**, das allen PC-Benutzern verdeutlicht werden sollte. Auf keinen Fall dürfen Computer ohne eine sorgfältige Bereinigung der Festplatte ausgesondert bzw. in fremde Hände gegeben werden. Ein erneutes Formatieren oder die Löschung der Partition reicht nicht aus. Es muss ein Tool, z. B. DataEraser (www.ontrack.de), eingesetzt werden, das die Festplatte vollständig neu beschreibt. Nur so kann gewährleistet werden, dass die Daten auf der Festplatte nicht rekonstruiert werden können.

Das Löschen von Ordnern und Dateien verschiebt diese zunächst in den Papierkorb. Sobald Sie die Objekte des Papierkorbs über die Funktion PAPIERKORB LEEREN entfernen, sind die Objekte (Ordner und Dateien) mit den Funktionen von Windows 2000 nicht wiederherstellbar.

Es gib allerdings einfach zu bedienende Tools mit grafischer Oberfläche (www.quetek.com), die bereits gelöschte Ordner und Dateien wiederherstellen können. Der Zeitraum der vollständigen Wiederherstellung der Objekte hängt von der freien Festplattenkapazität ab. Je größer die freie Festplattenkapazität, desto länger ist der Zeitraum der Wiederherstellung gelöschter Objekte.

Sollten Sie Systeme aussondern, setzen Sie ein professionelles Bereinigungswerkzeug (www.ontrack.de) ein, das den Datenträger insgesamt neu beschreibt. Ein Löschen, Formatieren oder Partitionieren reicht nicht aus (siehe Kapitel 13)!

11.6 Sicherheitscheck

- *Führen Sie in regelmäßigen Abständen eine **Sicherheitsanalyse** durch.*
- *Beachten Sie, dass nur **Teilbereiche** der Konfiguration in die Sicherheitsanalyse einbezogen werden.*
- *Verwenden Sie eine **Vorlage**, die Sie nach Ihren Anforderungen anpassen und unter einem neuen Namen abspeichern.*
- *Überprüfen Sie, inwieweit sich **Sicherheitseinstellungen** verändert haben.*
- *Bei Abweichungen in den vorgegebenen Sicherheitseinstellungen sollten Sie die **Ursache** klären.*
- *Eine Sicherheitskonfiguration sollten Sie zunächst auf einem **Testsystem** durchführen.*

- *Stellen Sie sicher, dass Ihnen alle Einstellungen der importierten Sicherheitsvorlage **bekannt** sind, die Sie für die automatische Konfiguration verwenden wollen.*

- *Verwenden Sie das Freewaretool **DumpSec** für die Kontrolle der administrativen Einstellungen im Bereich der Benutzer- und Gruppenverwaltung sowie für die Zuweisung von Freigabe- und NTFS-Berechtigungen.*

- *Beachten Sie, dass über **aktive** Disketten-, CD-ROM-Laufwerke und über USB-Ports mittels Speichersticks die **Datensicherheit** erheblich beeinträchtigt werden kann.*

- *Setzen Sie ein Tool ein, mit dem die **Schnittstellen** des Computers benutzerbezogen deaktiviert werden können.*

- *Berücksichtigen Sie, dass einige Systemdateien im **laufenden Betrieb** nicht defragmentiert werden können. Setzen Sie hierfür ein Tool ein, das die entsprechenden Dateien während der Bootphase defragmentiert.*

- *Weisen Sie die Benutzer darauf hin, dass **gelöschte** Dateien **wiederhergestellt** werden können.*

- *Setzen Sie ein Tool für die **Festplattenbereinigung** ein, wenn Sie den Computer aussondern bzw. dauerhaft in fremde Hände geben.*

12 Systemwiederherstellung

In diesem Kapitel erfahren Sie,

- über welche Funktionen das Datensicherungsprogramm *NTBackup* verfügt,
- etwas über den Unterschied zwischen den unterstützten Datensicherungsmethoden,
- welche Bedeutung die erweiterten Startoptionen haben,
- mit welchen Werkzeugen ein Windows 2000-System repariert werden kann,
- welche Funktionen die Notfalldiskette enthält,
- wie die Active Directory-Datenbank strukturiert ist,
- welche Verfahren für die Reparatur und Wiederherstellung einer Active Directory-Datenbank eingesetzt werden können und
- etwas über den Unterschied zwischen einer Online- und Offline-Defragmentierung der Active Directory-Datenbank.

12.1 Windows Backup

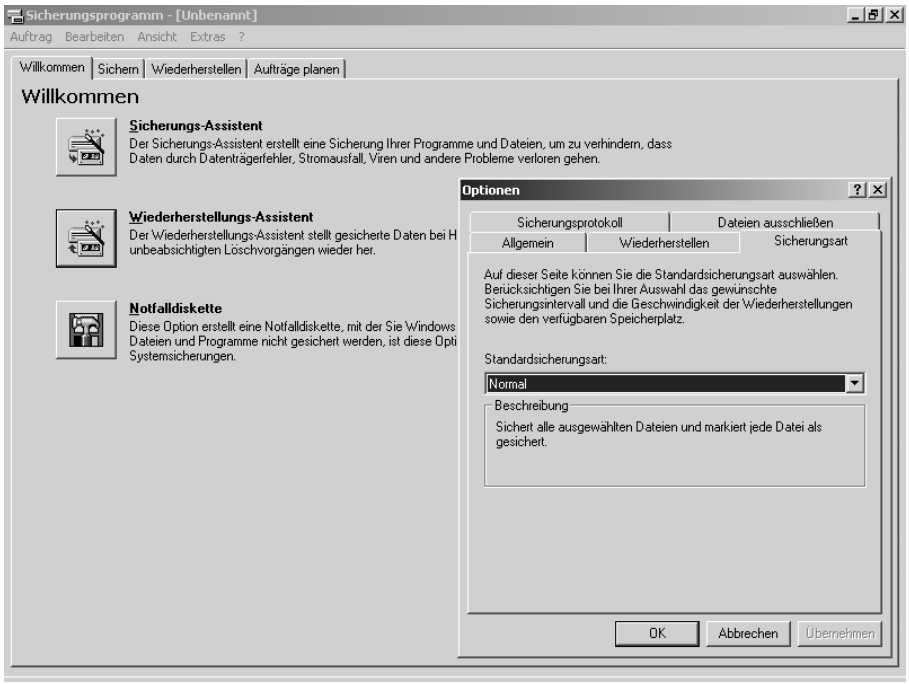
NTBackup.exe bzw. *Windows Backup* wird über START-PROGRAMME-ZUBEHÖR-SYSTEMPROGRAMME-SICHERUNG aufgerufen und verfügt über eine bedienerfreundliche Benutzeroberfläche einschließlich eines Assistenten zum Sichern und Wiederherstellen von Dateien.

Windows Backup unterstützt folgende Funktionen:

- das Sichern ausgewählter Dateien und Ordner auf der Festplatte,
- das Wiederherstellen der archivierten Dateien und Ordner auf der Festplatte oder auf einem anderen verfügbaren Datenträger,
- das Erstellen einer Notfalldiskette, mit der die Systemdateien repariert werden können, wenn diese beschädigt oder versehentlich gelöscht wurden,
- die Datensicherung auf Datenträger der im Netzwerk befindlichen Computer,

- die Datensicherung der Systemstatusdaten des Computers; hierzu gehören die Systemdateien, die Registrierung, die Komponentendienste, die Active Directory-Datenbank, der Dateireplikationsdienst SYSVOL und die Datenbank der Zertifikatsdienste,
- das Planen einer automatisierten Datensicherungen über einen TASKPLANER.

Darüber hinaus können zum Sichern von Dateien Bandlaufwerke und/oder andere Speichergeräte verwendet werden. Als Sicherungsmedium werden logische Laufwerke, Wechseldatenträger, beschreibbare CD-ROM oder „normale“ Datensicherungsbänder unterstützt.



Windows Backup – Sicherungsart

Windows Backup unterstützt fünf Sicherungsmethoden:

- **Kopie-Sicherung**

  Bei der *Kopie-Sicherung* werden alle ausgewählten Dateien kopiert, ohne dass die Dateien als gesichert markiert werden. Diese Sicherungsmethode ist dann sinnvoll, wenn außerplanmäßig neben einer anderen Sicherungsmethode Dateien gesichert werden sollen.

- **Tägliche Sicherung**

  Bei einer *täglichen Sicherung* werden alle ausgewählten Dateien kopiert, die an dem Tag geändert wurden, an dem die Sicherung ausgeführt wird. Die gesicherten Dateien werden nicht als gesichert gekennzeichnet.

- **Differenzielle Sicherung**

  Bei der *differenziellen Sicherung* werden Dateien kopiert, die seit der letzten Sicherung des Typs *Normal* oder *Inkrementell* erstellt bzw. geändert wurden. Die gesicherten Dateien werden nicht als gesichert gekennzeichnet.

  Wenn Sie eine Kombination aus normaler und differenzieller Sicherung durchführen, ist es zum Wiederherstellen von Dateien und Ordnern erforderlich, dass Ihnen die letzte normale sowie die letzte differenzielle Sicherung zur Verfügung steht.

- **Inkrementelle Sicherung**

  Bei einer *inkrementellen Sicherung* werden nur die Dateien gesichert, die seit der letzten Sicherung des Typs *Normal* oder *Inkrementell* erstellt bzw. geändert wurden. Dabei werden die gesicherten Dateien als solche markiert.

  Wenn Sie eine Kombination aus normalen und inkrementellen Sicherungen verwenden, benötigen Sie zum Wiederherstellen Ihrer Daten zum einen den letzten normalen Sicherungssatz und zum anderen alle inkrementellen Sicherungssätze.

- **Normale Sicherung**

  Bei der *normalen Sicherung* werden alle ausgewählten Dateien kopiert und als gesichert markiert.

  Beim normalen Sicherungsverfahren benötigen Sie lediglich die aktuelle Sicherung, um sämtliche Dateien wiederherzustellen. Das normale Sicherungsverfahren führen Sie aus, wenn Sie das erste Mal einen Sicherungssatz erstellen. Alle nachfolgenden Sicherungen können vom Typ *Inkrementell* sein.

Die Datensicherung unter Einsatz einer Kombination von normalen und inkrementellen Sicherungen belegt den **geringsten** Speicherplatz und stellt die **schnellste** Sicherungsmethode dar.

Die Wiederherstellung der Dateien nimmt jedoch möglicherweise **geraume Zeit** in Anspruch, da der Sicherungssatz auf mehrere Datenträger oder Bänder verteilt sein kann.

Die **Kombination** aus einer normalen und differenziellen Sicherung ist hingegen zeitaufwendiger, insbesondere wenn sich die Daten häufig ändern. Andererseits können die Daten schneller und einfacher wiederhergestellt werden, da der Sicherungssatz in der Regel nur auf wenigen Datenträgern bzw. Bändern vorliegt.

Empfohlen wird jedoch, täglich auf Tagesbändern eine normale Sicherung durchzuführen. Es ergeben sich somit **fünf Tagesbänder**, auf denen sich jeweils eine Vollsicherung befindet. Eine evtuelle Wiederherstellung kann dann unproblematisch über ein einzelnes Band durchgeführt werden.

Folgendes sollten Sie bei der Datensicherung beachten:

- *Eine sorgfältige Planung ermöglicht die schnelle Wiederherstellung im Falle eines Datenverlusts.*
- *Sofern personell möglich, sollten Sie einem Benutzer Sicherungsrechte und einem anderen Benutzer Wiederherstellungsrechte gewähren.*
- *Schulen Sie die entsprechenden Mitarbeiter in der Durchführung ihrer Aufgaben.*
- *Führen Sie nach Möglichkeit nur Vollsicherungen über die Sicherungsmethode* NORMALE SICHERUNG *durch.*
- *Erstellen Sie für jede Sicherung ein Sicherungsprotokoll. Drucken Sie die Protokolle stets aus, um das Auffinden und eventuelles Wiederherstellen bestimmter Dateien zu vereinfachen. Wenn das Band mit dem Katalog des Sicherungssatzes beschädigt sein sollte, können Sie auf das gedruckte Protokoll zurückgreifen, um eine Datei zu suchen.*
- *Halten Sie für jeden Wochentag ein Datensicherungsband bereit. Darüber hinaus sollte ein Wochensicherungsband außerhalb des Arbeitsplatzes in einer angemessen gesicherten Umgebung (Schließfach der Bank) aufbewahrt werden.*
- *Führen Sie zu Testzwecken regelmäßig Wiederherstellungen durch, um sicherzustellen, dass die Dateien fehlerfrei gesichert wurden. Auf diese Weise werden ggf. Hardwareprobleme erkannt, die anhand von Softwareprüfungen nicht ermittelt werden können.*

12.2 Windows 2000-Reparatur

12.2.1 Abgesicherter Modus

Beim abgesicherten Modus wird Windows 2000 mit einem **minimalen** Satz von Treibern und Diensten gestartet. Wenn Windows 2000 beispielsweise aufgrund installierter Gerätetreiber oder Softwareprogramme nicht mehr gestartet werden kann, können über den abgesicherten Modus die betreffende Software bzw. die Treiber entfernt werden. Der abgesicherte Modus führt nicht in allen Fällen zum Erfolg. Dies gilt insbesondere dann, wenn die Systemdateien beschädigt wurden oder fehlen.

Abgesicherter Modus

Windows 2000 im abgesicherten Modus starten!

1. *Starten Sie den Computer neu, um die erweiterten Startoptionen zu aktivieren.*
2. *Drücken Sie während der Bootphase die Funktionstaste F8, sobald am untersten Bildschirmrand die Meldung erscheint: PROBLEMBEHANDLUNG UND ERWEITERTE STARTOPTIONEN: F8 TASTE DRÜCKEN.*
3. *Wählen Sie eine der drei Optionen:*
   - *abgesicherter Modus,*
   - *abgesicherter Modus mit Netzwerktreibern oder*
   - *abgesicherter Modus mit Eingabeaufforderung.*

4. *Nachdem Windows 2000 im abgesicherten Modus hochgefahren ist, können Sie nach der Anmeldung unter dem lokalen Administratorkonto das System eingeschränkt administrieren.*

12.2.2 Verzeichnisdienstwiederherstellung

Die Reparaturfunktion VERZEICHNISDIENSTWIEDERHERSTELLUNG ist ebenfalls über die erweiterten Startoptionen ausführbar. Nach Auswahl dieser Funktion werden automatisch der **Verzeichnisdienst** (Active Directory-Datenbank) und der bzw. die **Datenträger** (Festplatte) überprüft und ggf. vorhandene Fehler beseitigt. Anschließend wird das System mit Ausnahme des Active Directory vollständig gestartet. Unter der *Systemsteuerung* können die Systemprogramme für die weitere Fehlerdiagnose und Fehlerbehebung des Active Directory ausgeführt werden.

Beachten Sie, dass die Wiederherstellung der Systemstatusdateien von einer Datensicherung nur im VERZEICHNISDIENSTWIEDERHERSTELLUNGSMODUS durchgeführt werden kann (siehe Tzn. 12.3.2 und 12.3.3).

12.2.3 Letzte als funktionierend bekannte Konfiguration

Windows 2000 verwaltet einen Teil der Registrydaten als **Sicherungskopie** (Controlset bzw. Profil) auf der Festplatte. Sollte die Situation eintreten, dass nach einer Installation von Software Windows 2000 abstürzt und nicht fehlerfrei wieder hochfährt, kann auf die Sicherungskopie der Konfiguration zurückgegriffen werden. Über die ERWEITERTEN STARTOPTIONEN wird mit der Option LETZTE ALS FUNKTIONIEREND BEKANNTE KONFIGURATION das System wiederhergestellt. Alle Systemkonfigurationsänderungen, die seit dem **letzten** erfolgreichen Starten durchgeführt wurden, gehen dabei verloren.

Letzte funktionierende Konfiguration wiederherstellen!

1. *Starten Sie das System neu und rufen Sie die ERWEITERTEN STARTOPTIONEN mit der Funktionstaste F8 auf.*

2. *Wählen Sie die Option LETZTE ALS FUNKTIONIEREND BEKANNTE KONFIGURATION aus.*

3. *Es erscheint ein Auswahlmenü mit den verfügbaren Sicherungskopien (Profilen). Standardmäßig wird nur ein Profil verwaltet.*

4. *Nachdem Sie das Profil mit der ENTER-TASTE ausgewählt haben, startet das System mit der letzten funktionierenden Konfiguration.*

12.2.4 Reparaturkonsolen der Windows 2000-Installations-CD

Sofern **schwerwiegende** Fehler vorliegen, kann das System über den REPARATURMODUS der Windows 2000-Installations-CD repariert werden. Dieser Modus sollte verwendet werden, wenn z. B. der Bootsektor oder Systemdateien beschädigt sind. Wenn das System über die Installations-CD gebootet wird, wird zunächst die Hardwareinstallation untersucht. Im Anschluss erscheint ein Menü, über das mit der R-Taste in den REPARATURMODUS gewechselt werden kann. Es stehen zwei Konsolen für die Reparatur zur Verfügung:

- die Notfallreparaturkonsole und
- die Wiederherstellungskonsole.

Windows 2000 über die Installations-CD reparieren!

1. *Definieren Sie im BIOS die Bootreihenfolge und wählen Sie das CD-ROM-Laufwerk als 1. Bootlaufwerk.*

2. *Legen Sie die Installations-CD in das CD-ROM-Laufwerk und starten Sie neu.*

3. *Nach dem Bootvorgang von der CD-ROM wird zunächst die Hardwareinstallation untersucht. Danach erscheint ein Auswahlmenü, in dem Sie die R-Taste für BESCHÄDIGTE WINDOWS 2000-INSTALLATION REPARIEREN betätigen.*

4. *Es erscheint ein weiteres Auswahlmenü, in dem Sie entweder durch Betätigung der K-Taste die WIEDERHERSTELLUNGSKONSOLE oder über die R-Taste die NOTFALLREPARATURKONSOLE aufrufen.*

12.2.5 Notfallreparaturkonsole

Nach dem Aufruf der Notfallreparaturkonsole mit der R-Taste können folgende Bereiche überprüft und fehlerhafte Bereiche automatisch repariert werden:

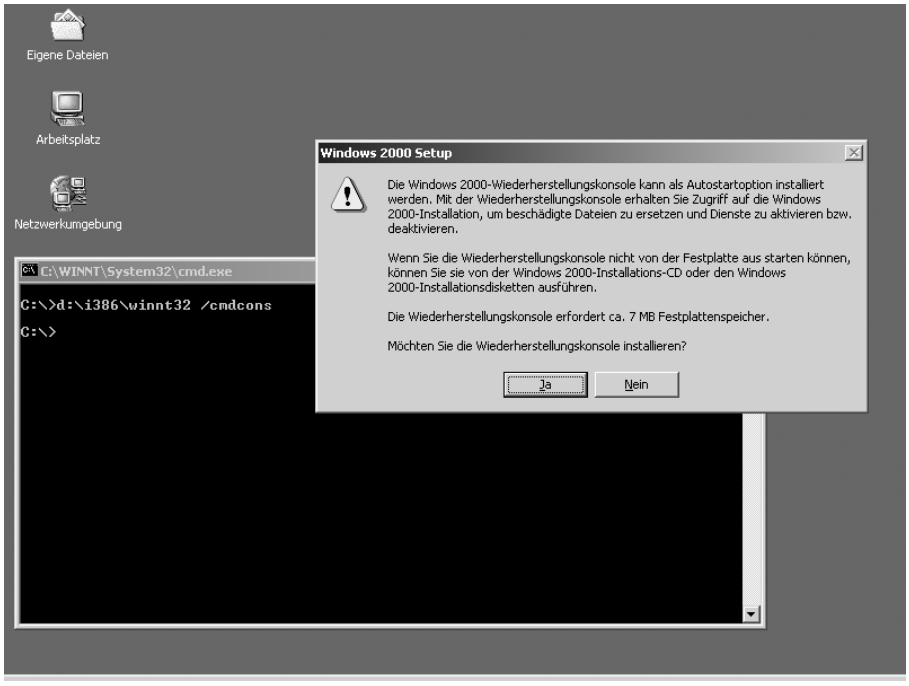
- Untersuchen der Startumgebung,

- Überprüfen der Windows 2000-Systemdateien,
- Untersuchen des Startsektors.

Der Administrator kann entweder über die Betätigung der S-Taste alle Reparaturoptionen prüfen lassen oder über die M-Taste einzelne Bereiche für die Überprüfung selektieren. Zusätzlich erscheint eine Aufforderung zum Einlegen einer **Notfalldiskette** in das Diskettenlaufwerk (siehe Tz. 12.2.7). Wenn **keine** Notfalldiskette vorliegt, versucht Windows 2000 über die auf der Festplatte verfügbaren Dateien im Ordner <Stammverzeichnis:\winnt\repair> die fehlerhaften Bereiche zu beheben.

12.2.6 Wiederherstellungskonsole

Die WIEDERHERSTELLUNGSKONSOLE wird erst nach Auswahl des zur reparierenden Betriebssystems (in der Regel 1 = C:\Winnt, Eingabe von 1 erforderlich) und nach Eingabe des Administratorkennwortes aufgerufen. Die WIEDERHERSTELLUNGSKONSOLE ist ein **Befehlszeilenprogramm**, mit dem Systemfehler mithilfe eines eingeschränkten Befehlssatzes behoben werden können. Es können z. B. Dienste gestartet und beendet, Laufwerke formatiert, Dateien auf dem lokalen Laufwerk bearbeitet und zahlreiche weitere Systemaufgaben ausgeführt werden.



Wiederherstellungskonsole in das Bootmenü installieren.

Die WIEDERHERSTELLUNGSKONSOLE sollte insbesondere dann eingesetzt werden, wenn **Systemfehler** nicht mithilfe der NOTFALLREPARATURKONSOLE behoben werden können. Sie kann auf zwei Arten gestartet werden:

- Aufruf über die Windows 2000-Installations-CD (siehe Tz. 12.2.4) oder
- Installation auf der Festplatte und Einrichtung einer Option in das STARTMENÜ über die Windows 2000 Installations-CD mit dem Befehl `<CD-ROM-Laufwerk:\i386\Winnt32 /cmdcons>`.

Mit der Installation der WIEDERHERSTELLUNGSKONSOLE wird auf der Festplatte ein Ordner <Stammverzeichnis:\CMDCONS> angelegt. Er enthält Dateien über die Beschaffenheit des Partitionsbootsektors (*bootsect.dat*), wesentliche Systemdateien für die Hardwareerkennung sowie den Befehlsinterpreter. Die Datei *bootsect.dat* stellt eine Standardmethode zum Laden eines alternativen Betriebssystems dar. Es wird eine Option mit dem Verweis auf die *bootsect.dat* im Startmenü eingetragen.

Inhalt der Datei *boot.ini* mit der Windows 2000-Wiederherstellungskonsole:

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(2)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(2)\WINDOWS="Windows .NET Server, Enterprise" /fastdetect
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Microsoft Windows 2000 Server" /fastdetect
C:\CMDCONS\BOOTSECT.DAT="Microsoft Windows 2000-Wiederherstellungskonsole" /cmdcons
```

Die WIEDERHERSTELLUNGSKONSOLE stellt u. a. folgende Befehle zur Verfügung:

attrib	ändert die Attribute einer Datei oder eines Verzeichnisses
batch	führt die Befehle aus, die in einer Textdatei aufgeführt sind
bootcfg	die Datei *boot.ini* lässt sich auswerten und bearbeiten
chdir (cd)	zeigt den Namen des aktuellen Ordners an oder wechselt den aktuellen Ordner
chkdsk	überprüft einen Datenträger und zeigt einen Statusbericht an

cls	löscht die Bildschirmanzeige
copy	kopiert eine einzelne Datei in einen anderen Pfad
delete (del)	löscht eine oder mehrere Dateien
dir	zeigt eine Liste der Dateien und Unterordner in einem Ordner an
disable	deaktiviert einen Systemdienst oder einen Gerätetreiber
diskpart	erstellt bzw. löscht Partitionen
enable	startet oder aktiviert einen Systemdienst oder einen Gerätetreiber
exit	beendet die Wiederherstellungskonsole und startet den Computer neu
expand	extrahiert eine Datei aus einer komprimierten Datei
fixboot	schreibt einen neuen Partitionsbootsektor auf die Systempartition
fixmbr	repariert den MBR (Master Boot Record) des Standarddatenträgers
format	formatiert einen Datenträger
help	zeigt eine Liste der Befehle an, die in der Wiederherstellungskonsole zur Verfügung stehen
listsvc	zeigt eine Liste der auf dem Computer verfügbaren Dienste und Treiber an
logon	meldet sich bei einer Windows 2000-Installation an
map	zeigt die Laufwerkzuordnung, Dateisystemtypen, Datenträgergrößen und Zuordnungseinheiten an, die derzeit aktiv sind
mkdir (md)	erstellt ein Verzeichnis
more	zeigt eine Textdatei an
rename (ren)	benennt eine einzelne Datei um
rmdir (rd)	löscht ein Verzeichnis
set	zeigt Umgebungsvariablen der Wiederherstellungskonsole an und ändert diese

systemroot	setzt den Systemordner auf die Variable <%systemroot%>
type	zeigt eine Textdatei an

Windows 2000-Wiederherstellungskonsole installieren!

1. *Starten Sie Ihr Windows 2000-System.*
2. *Nachdem Sie sich als Administrator angemeldet haben, rufen Sie die Eingabeaufforderung über AUSFÜHREN und nach Eingabe des Befehls CMD auf.*
3. *Legen Sie die Windows 2000-Installations-CD in das CD-ROM-Laufwerk und geben Sie den Befehl* `<D:\i386\winnt32 /cmdcons>` *ein (D: ist in diesem Beispiel der Laufwerkbuchstabe des CD-ROM-Laufwerkes).*
4. *Es erscheint ein Fenster mit der Abfrage, ob die Installation der WIEDERHERSTELLUNGSKONSOLE durchgeführt werden soll. Bestätigen Sie mit JA.*
5. *Nach Abschluss der Installation müssen Sie das System neu starten und über das STARTMENÜ die WIEDERHERSTELLUNGSKONSOLE aufrufen.*

12.2.7 Notfalldiskette

Die von Windows NT her bekannte Notfalldiskette hat sich unter Windows 2000 **bedeutend** verändert. Bei NT enthielt die Notfalldiskette eine komprimierte Kopie aller Dateien in der Registry. Die Windows 2000-Notfalldiskette enthält hingegen nur noch **drei Dateien**:

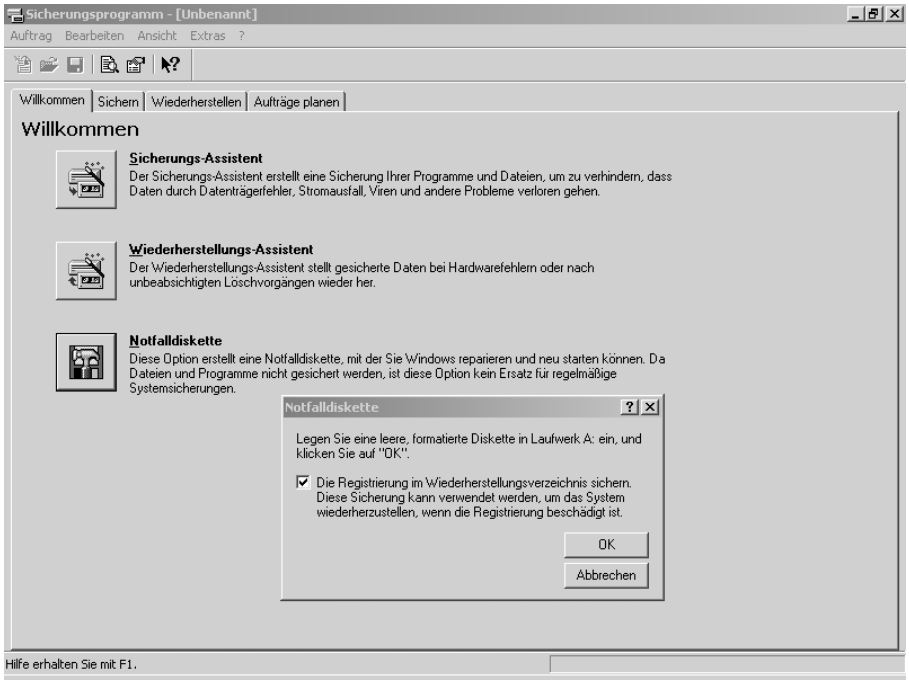
autoexec.nt und config.nt	dienen der Initialisierung von einem virtuellen DOS-Modul
setup.log	beinhaltet eine Liste der Dateien, die während der Installation von der CD kopiert wurden, sowie eine Kennung, über die festgestellt werden kann, ob die Dateien modifiziert wurden

Die Notfalldiskette ist **nicht bootfähig**, sondern sie wird in Verbindung mit der Reparaturoption der Windows 2000-Installations-CD benutzt. Mithilfe der Notfalldiskette können folgende Fehler behoben werden:

- Reparatur einer Multibootkonfiguration,

- Reparatur eines beschädigten Masterbootrecords (MBR) oder Partitionsbootsektors,
- Ersetzung fehlender oder falscher Windows 2000-Systemdateien.

Von diesen Reparaturfällen sind die ersten beiden über die WIEDERHERSTELLUNGSKONSOLE einfacher zu bearbeiten. Insofern ist die Reparatur von Systemdateien der einzige wirkliche Grund für das Erstellen einer Notfalldiskette. Sie kann mit dem Windows Backup-Programm erstellt werden.



Windows Backup – Notfalldiskette erstellen

Eine Notfalldiskette erstellen!

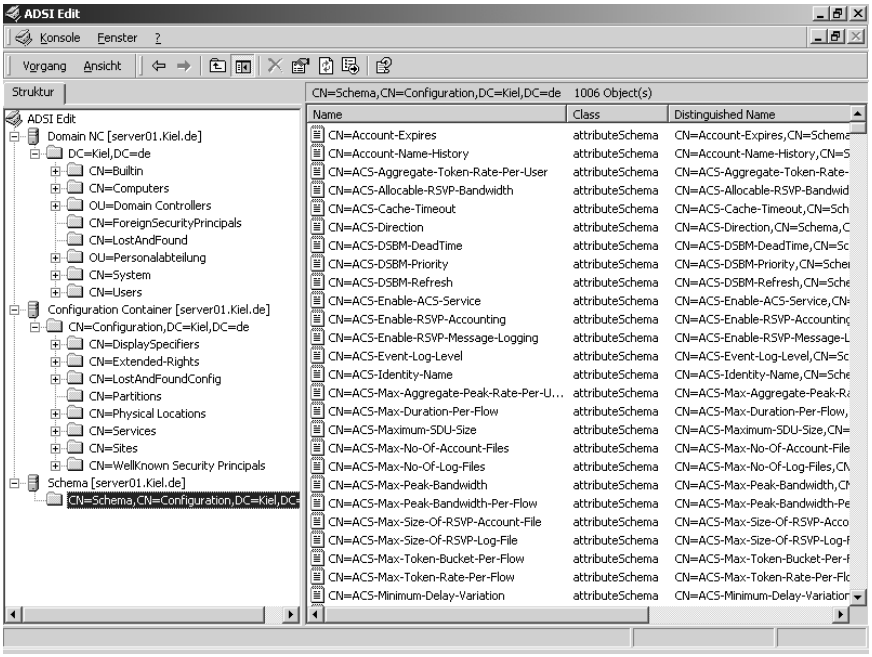
1. *Starten Sie das Backup-Programm über START-PROGRAMME-ZUBEHÖR-SYSTEMPROGRAMME-SICHERUNG.*
2. *Wählen Sie aus dem Menü EXTRAS die Option NOTFALLDISKETTE ERSTELLEN. Das Fenster NOTFALLDISKETTE öffnet sich.*
3. *Selektieren Sie die Option DIE REGISTRIERUNG IM WIEDERHERSTELLUNGSVERZEICHNIS SICHERN und klicken Sie auf OK. Die Registrierung wird nicht auf die Notfalldiskette, sondern in den Ordner <Stammlaufwerk:\winnt\repair\regback> kopiert. Ohne eine aktuelle Kopie dieser Dateien kann ein System nach Verlust oder Beschädigung der Registry nicht mehr repariert werden!*
4. *Wenn die Registrydateien in den entsprechenden Ordner kopiert und die drei*

Konfigurationsdateien auf die Notfalldiskette geschrieben sind, wird im Fenster NOTFALLDISKETTE eine erfolgreiche Ausführung der Aufgaben angezeigt.

5. *Bewahren Sie die Notfalldiskette an einem sicheren Ort auf. Sie wird ausschließlich in Verbindung mit der Notfallreparaturkonsole der Windows 2000-Installations-CD benötigt (siehe Tz. 12.2.5).*

12.3 Verwaltung der Active Directory-Datenbank

12.3.1 Active Directory-Datenbankstrukturen



ADSI Edit, Active Directory-Datenbank intern

Die Active Directory-Datenbank ntds.dit besteht aus drei unabhängigen Partitionen (sog. Namenskontexte) mit voneinander unabhängigen Replikationsmechanismen. Wenn sich beispielsweise Objekte der Schemapartition verändern, wird nur diese zwischen allen Domänencontrollern innerhalb der Domänengesamtstruktur repliziert. Die drei Partitionen können mit dem Programm *ADSI Edit* aus den Support-Tools sichtbar und ggf. auch geändert werden.

- **Domänenpartition**

  Domänendaten bieten Informationen zu den in einer Domäne enthaltenen Objekten wie Kontakte, Benutzer, Gruppen, OE und Computerkonten sowie veröffentlichte Ressourcen wie Drucker und Freigaben. Wird z. B. ein Benutzerkonto eingerichtet, wird in der *Domänenpartition* ein User-Objekt sowie die dazugehörigen Attributdaten gespeichert.

- **Konfigurationspartition**

  Die *Konfigurationspartition* enthält die Topologie der gesamten Verzeichnisstruktur. Sie beinhaltet die Domänenstrukturen, die Standorte der Domänencontroller sowie den Globalen Katalog.

- **Schemapartition**

  In der *Schemapartition* wird die formelle Definition aller Objekt- und Attributdaten einer Gesamtstruktur (Domänenwald bzw. Forest) festgehalten. Windows 2000 Server beinhaltet ein Standardschema, in dem zahlreiche Objekttypen wie Benutzer- und Computerkonten, Gruppen, Domänen, Organisationseinheiten und Sicherheitsrichtlinien definiert sind. Administratoren können das Schema erweitern, indem sie neue Objekte hinzufügen. Schemaobjekte sind durch Zugriffssteuerungslisten geschützt, die sicherstellen, dass das Schema nur von autorisierten Benutzern geändert werden kann.

Ein *globaler Katalog-Server* (Global Catalog, GC) speichert neben den drei genannten Partitionen eine **Untermenge** der Domänenpartition von jeder anderen Domäne der Gesamtstruktur.

Active Directory besitzt ein eigenes **Datenbankmodul** mit der Bezeichnung **ESE** (Extensible (erweiterbare) Schema Engine). ESE verwendet ein Konzept aus **Transaktionen** und **Protokolldateien**, um die Integrität der Active Directory-Datenbank sicherzustellen.

Eine Active Directory-Datenbank enthält folgende Dateien:

- **Ntds.dit**

  Diese einzelne Datei ist die Active Directory-Datenbank, in der alle Objekte gespeichert werden. DIT steht für DIRECTORY INFORMATION TREE und stammt von dem X.500 Standard. Der Standardspeicherort ist <Stammverzeichnis:\winnt\ntds>.

  Die Active Directory-Datenbank sollte auf einer eigenständigen Partition mit der Sicherheitsstufe RAID 5 gespeichert werden.

- **Edb.log**

Dies ist eine Transaktionsprotokolldatei, in der Veränderungen der Datenbank zwischengespeichert werden. Diese Datei ist exakt 10 MB groß. Wenn die Datei voll ist, wird sie in Edbnnnnn.log umbenannt, wobei nnnnn eine Zahl ist, die bei 00001 aufsteigend beginnt.

Die Transaktionsprotokolldateien Edb.log und Edbnnnnn.log sollten ebenfalls auf einer separaten Partition mit der Sicherheitsstufe RAID 1 (Spiegelung) gespeichert werden.

- **Edb.chk**

  Die Datei ist eine so genannte Prüfpunktdatei, die den Status zwischen dem Arbeitsspeicher und der Datenbankdatei auf der Festplatte verwaltet. Sie gibt den Startpunkt in der Transaktionsprotokolldatei an, ab dem die Informationen nach einem Fehler wiederhergestellt werden müssen.

- **Res1.log und Res2.log**

  Dies sind reservierte Transaktionsprotokolldateien. Jede dieser Dateien ist exakt 10 MB groß. Der reservierte Festplattenplatz dient vorbeugend dazu, den Transaktionsprotokolldateien ausreichenden Speicherplatz zur Verfügung zu stellen.

Wenn Active Directory-Daten geändert werden, läuft ein Datenbankänderungsvorgang durch ESE wie folgt ab:

- ESE lagert die zu ändernden Daten in den **Arbeitsspeicher** (RAM) aus. Durch die Zwischenspeicherung im RAM muss ESE nicht ständig auf die Festplatte zugreifen. Das führt zu weniger Schreibvorgängen auf der Festplatte und beschleunigt somit erheblich die Leistung.

- Danach sichert ESE die Transaktion in der Tranksaktionsprotokolldatei **Edb.log** durch einen entsprechenden Eintrag. Wenn ESE das Ende einer Transaktionsprotokolldatei erreicht, wird Edb.log in **Edbnnnnn.log** umbenannt und eine neue Edb.log erstellt. „Alte“ Protokolldateien (Edbnnnnn.log), die nicht mehr benötigt werden, werden automatisch gelöscht.

- ESE schreibt die im RAM gespeicherte Änderung in die Datenbankdatei **Ntds.dit** auf der Festplatte.

- Abschließend aktualisiert ESE die Prüfpunktdatei **Edb.chk**. Damit wird festgehalten, dass die Transaktion in der Protokolldatei Edb.log bzw. Edbnnnnn.log an die Datenbank übergeben wurde.

12.3.2 Sichern der Active Directory-Datenbank

Windows Backup kann zur Datensicherung für die Active Directory-Datenbank und deren Transaktionsdateien im **laufenden** Betrieb eingesetzt werden. Die Active Directory-Datenbank ist ein Teil der Systemstatusdaten. Auf einem Domänencontroller umfassen die Systemstatusdaten folgende Komponenten:

- Active Directory-Datenbank,
- die Systemfreigabe SYSVOL (enthält Gruppenrichtlinien und Skripte),
- die Registrierung,
- die Startdateien einschließlich aller Systemdateien,
- die COM+ Class Registration Database,
- die Zertifikatdatenbank, wenn auf dem Server ein PKI installiert ist sowie
- Informationen des Clusterdienstes, wenn dieser installiert wurde.

Im Rahmen der Sicherung werden diese Systemkomponenten als **Systemstatusdaten** bezeichnet. Sie beinhalten ca. 2000 Dateien und benötigen ca. 300 MB Speicherkapazität. Bei Windows 2000 Professional umfassen die Systemstatusdaten lediglich die Registrierung, die COM+ Class Registration Database, die Systemstartdateien sowie die Zertifikatsdienstedatenbank, falls ein Zertifikatsserver eingesetzt wird.

Wenn auf dem Domänencontroller ein DNS-Server (Domain Name Service) installiert wurde, gehören zu den Systemstatusdaten außerdem die gesamten Daten der DNS-Zone.

Wenn Sie die Systemstatusdaten sichern oder wiederherstellen, werden alle Daten berücksichtigt, die für den entsprechenden Computer relevant sind. Es ist nicht möglich, einzelne Komponenten der Systemstatusdaten zu sichern oder wiederherzustellen. Der Grund hierfür liegt in den Abhängigkeiten zwischen den einzelnen Komponenten.

Windows Backup ist nicht in der Lage, die Systemstatusdaten von einem Remote-Domänencontroller zu sichern. Diese können jedoch mit einem speziellen Backupprogramm von Drittanbietern gesichert werden.

Die Systemstatusdaten von einem Domänencontroller beinhalten spezifische Eigenschaften, wie z. B. die Betriebsmasterfunktionen. Sie müssen daher für jeden Controller die Systemstatusdaten separat auf Bändern sichern.

12.3.3 Reparieren der Active Directory-Datenbank

Wenn die Active Directory-Datenbank aufgrund einer fehlerhaften Datenbankstruktur oder beschädigter Indexdateien nicht mehr funktioniert, kann ein **Reparaturvorgang** durchgeführt werden. Über den VERZEICHNISDIENSTWIEDERHERSTELLUNGSMODUS kann die Reparatur mit dem Programm *ntdsutil* über zwei Verfahren durchgeführt werden:

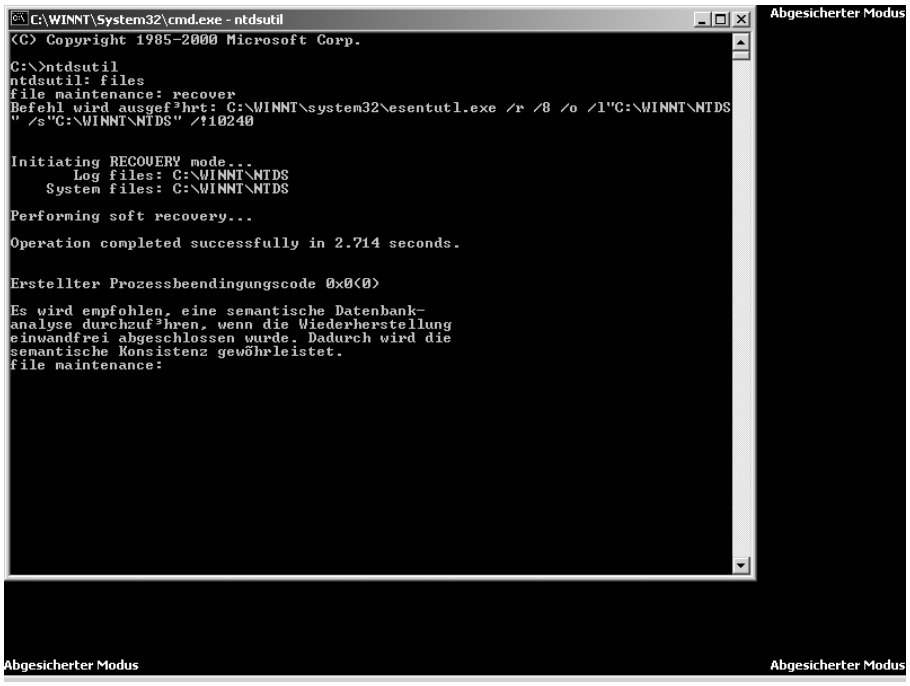
- *Recover* restauriert die Datenbank anhand der Protokoll- und Prüfpunktdateien.
- *Repair* überprüft die Datenbank und löscht alle beschädigten Objekte.

Active Directory-Datenbank reparieren!

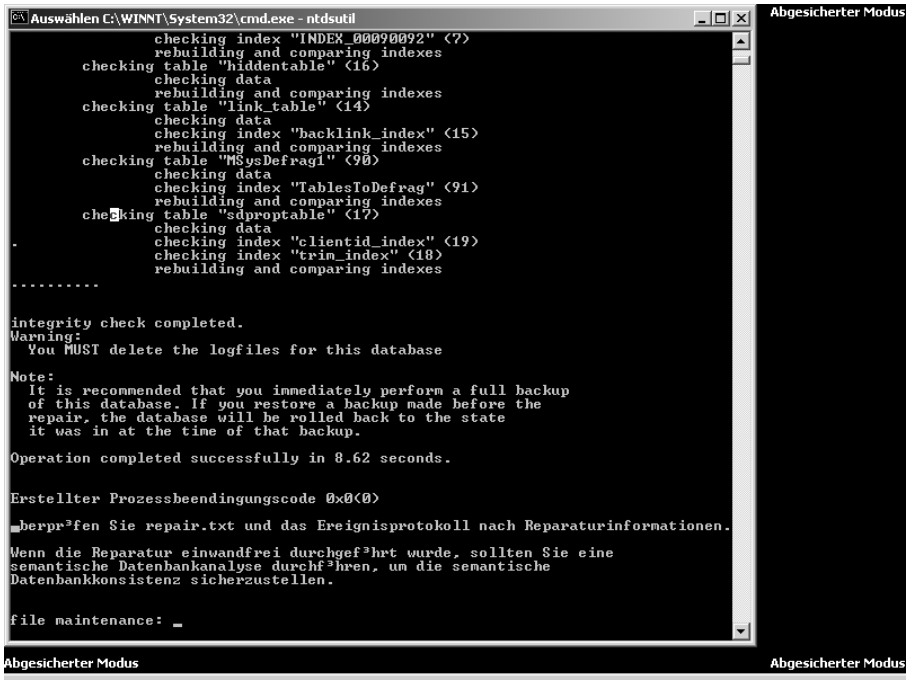
1. *Sichern Sie als Vorsichtsmaßnahme die Active Directory-Datenbank.*
2. *Starten Sie den Domänencontroller neu und aktivieren Sie über die Funktionstaste F8 die erweiterten Startoptionen.*
3. *Wählen Sie den* VERZEICHNISDIENSTWIEDERHERSTELLUNGSMODUS *und melden Sie sich unter dem lokalen Administratorkonto an.*
4. *Starten Sie das Programm* ***ntdsutil****, indem Sie in der Eingabeaufforderung* `ntdsutil` *eingeben.*
5. *Geben Sie den Befehl* `files` *ein, um die Befehlsebene* FILE MAINTENANCE *zu öffnen.*
6. *Durch die Eingabe von* `recover` *können Sie den Reparaturvorgang unter der Verwendung der Protokoll- und Prüfpunktdateien (siehe Abbildung) starten. Geben Sie* `repair` *ein, werden beschädigte Objekte aus der Datenbank entfernt (siehe Abbildung). Tritt während der Reparatur ein Problem auf, wird die entsprechende Fehlermeldung in die Datei repair.txt im Ordner <Stammverzeichnis:\winnt\ntds> geschrieben.*
7. *Verlassen Sie* ***ntdsutil****, indem Sie auf der Befehlsebene* `quit` *und danach nochmals* `quit` *eingeben.*

8. *Löschen Sie die Protokolldateien (edb.log, res1.log, res2.log) im Verzeichnis <Stammverzeichnis:\winnt\ntds>.*

9. *Starten Sie den Domänencontroller neu und überprüfen Sie, ob die Active Directory-Datenbank fehlerfrei ist.*



***ntdsutil* – Reparatur über den Befehl RECOVER**



***Ntdsutil* – Reparatur über den Befehl repair**

12.3.4 Wiederherstellen der Active Directory-Datenbank

Für die Wiederherstellung einer Active Directory-Datenbank gibt es zwei typische Situationen:

- Die Active Directory-Datenbank lässt sich nicht reparieren (siehe Tz. 12.3.3) und muss über die Datensicherung ersetzt werden.
- Es wurden versehentlich Objekte aus der Active Directory-Datenbank gelöscht, und die Datenbank wurde bereits auf alle in der Domäne installierten Domänencontroller repliziert.

In beiden Situationen ist für die Wiederherstellung einer Active Directory-Datenbank entscheidend, ob weitere Domänencontroller in der Domäne mit einer aktuellen Datenbank verfügbar sind.

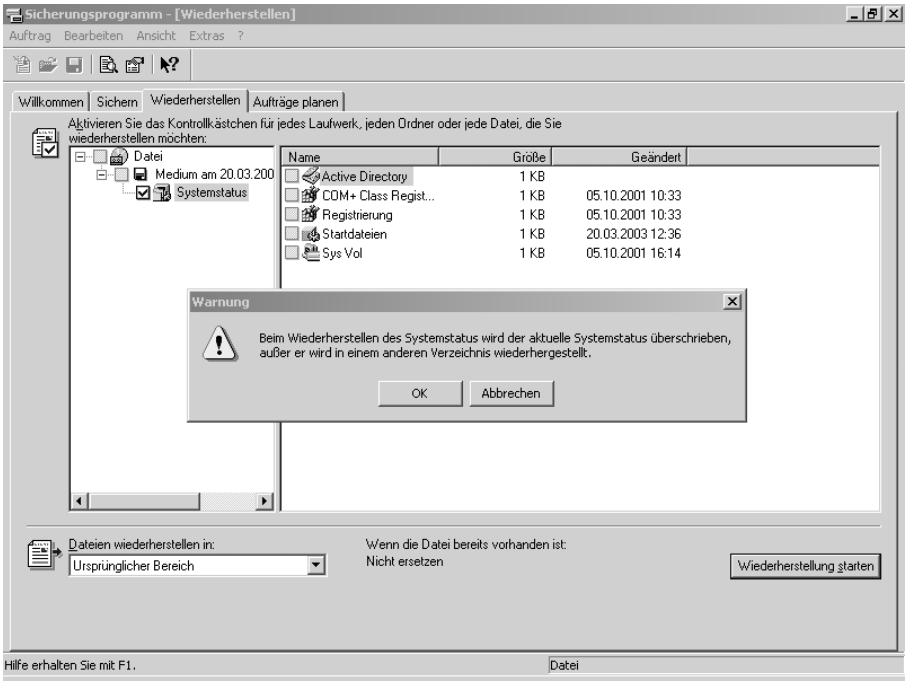
Defekte Active Directory-Datenbank wiederherstellen!

1. *Starten Sie den Domänencontroller neu und aktivieren Sie über die Funktionstaste F8 die erweiterten Startoptionen.*
2. *Wählen Sie den* VERZEICHNISDIENSTWIEDERHERSTELLUNGSMODUS *aus und melden Sie sich unter dem Administratorkonto an.*
3. *Starten Sie das Windows Backup-Sicherungsprogramm über* START-PROGRAMME-ZUBEHÖR-SYSTEMPROGRAMME-SICHERUNG.
4. *Wählen Sie die Registerkarte* WIEDERHERSTELLEN.
5. *Setzen Sie auf das Kontrollkästchen neben der Option* SYSTEMSTATUS *ein Häkchen. Es öffnet sich ein Fenster, in dem der Ort der Sicherungsdatei anzugeben ist. Dieser Vorgang kann einige Sekunden dauern, da nach einer entsprechenden Sicherungsdatei gesucht wird.*
6. *Klicken Sie auf* WIEDERHERSTELLUNG STARTEN. *Es öffnet sich ein Warnfenster, das auf das Überschreiben der Systemstatusdateien hinweist. Bestätigen Sie den Hinweis mit OK (siehe Abbildung).*
7. *Im nächsten Fenster* WIEDERHERSTELLUNG BESTÄTIGEN *wählen Sie ebenfalls OK, um die Wiederherstellung zu starten. Wenn der Vorgang abgeschlossen ist, klicken Sie auf* BERICHT, *um das Protokoll in Bezug auf die fehlerfreie Rücksicherung zu überprüfen (siehe Abbildung).*
8. *Werden im Protokoll Fehler angezeigt, die das Active Directory betreffen, beenden Sie den Vorgang, starten das System im normalen Modus und befolgen die Schritte 9 – 11).*

9. *Rufen Sie über START-AUSFÜHREN* `dcpromo` *auf, um den Domänencontroller herabzustufen. Im Anschluss daran installieren Sie mit* `dcpromo` *eine neue Active Directory-Datenbank und führen die Schritte von 1. beginnend erneut durch.*

10. *Schließen Sie das Fenster und beenden Sie das Sicherungsprogramm. Sie werden dann aufgefordert, das System neu zu starten.*

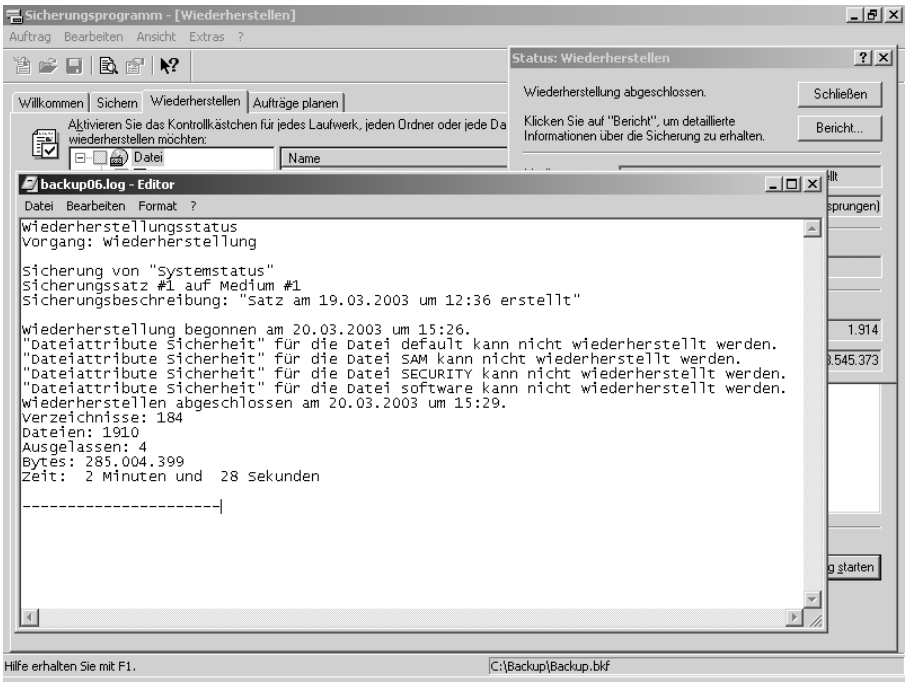
11. *Nach dem Neustart wird die reparierte Active Directory-Datenbank über die Replikation der in der Domäne integrierten weiteren Domänencontroller aktualisiert. Sind in der Domäne keine weiteren Domänencontroller verfügbar, enthält die Active Directory-Datenbank zumindest den Stand der letzten Datensicherung der Systemstatusdateien.*



Wiederherstellung - Systemstatusdateien überschreiben

Sie können eine Active Directory-Datenbank nicht aus einer Datensicherung wiederherstellen, die älter als 60 Tage ist. Ein Domänencontroller protokolliert gelöschte Objekte nur für diesen Zeitraum (Tombstone-Lebensdauer).

Sofern versehentlich Objekte in einer Active Directory-Datenbank gelöscht wurden, können diese nur dann wiederhergestellt werden, wenn die Objekte über die Datensicherung rekonstruiert werden können. Befinden sich weitere Domänencontroller in der Domäne, enthalten diese aufgrund der Replikation bereits den veränderten (gelöschten) Zustand.



Bericht über den Wiederherstellungsstatus

Wird eine Wiederherstellung einer Active Directory-Datenbank über eine Datensicherung durchgeführt, ist zu berücksichtigen, dass diese Datenbank über eine ältere **Versionsnummer** verfügt als die Datenbanken weiterer in der Domäne befindlichen Domänencontroller. Das hätte zur Folge, dass eine neuere Datenbank grundsätzlich immer ältere überschreibt. Die Versionsnummer der wiederhergestellten Datenbank muss also unmittelbar nach der Wiederherstellung mit dem Programm *ntdsutil* erhöht werden, um zu erreichen, dass die Replikation auf andere Domänencontroller von der wiederhergestellten Datenbank ausgeht. Dieses Verfahren wird unter Windows 2000 als a*utorisierende Wiederherstellung* bezeichnet.

Versehentlich gelöschte Objekte in der Active Directory-Datenbank wiederherstellen!

1. *Führen Sie die Schritte 1 – 7 der oben beschriebenen Wiederherstellung durch.*
2. *Starten Sie jedoch den Domänencontroller nach der erfolgreichen Wiederherstellung* ***nicht*** *neu.*
3. *Rufen Sie über* START-AUSFÜHREN `cmd` *(Eingabeaufforderung) auf und geben Sie* `ntdsutil` *ein.*
4. *Über das Programm ntdsutil können Sie nun weitere Befehle für die Administration der Active Directory-Datenbank eingeben.*

5. *Durch die Eingabe von* `help` *werden alle Befehle angezeigt.*

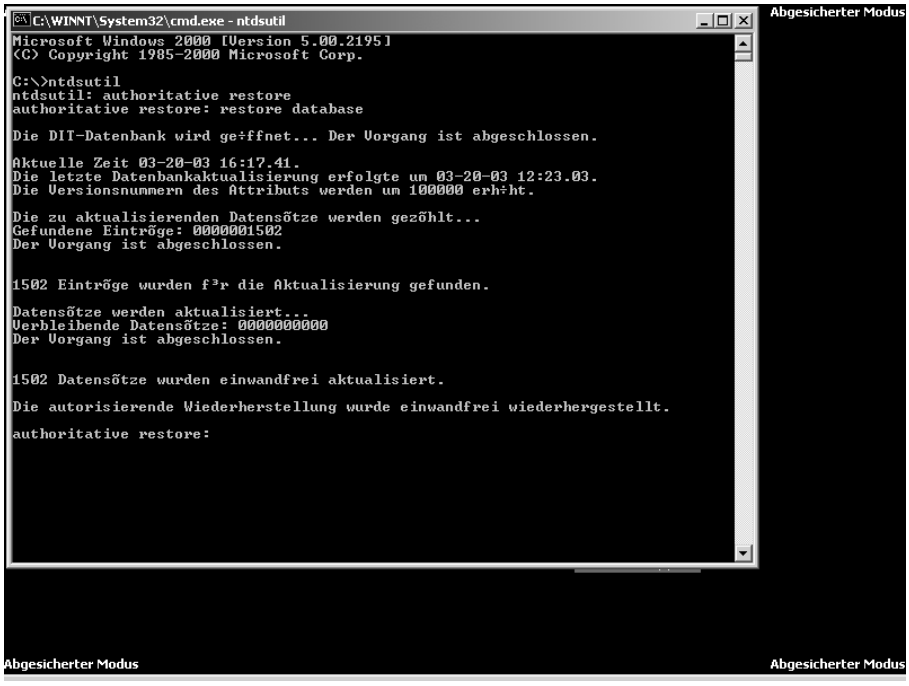
6. *Mit dem Befehl* `authoritative restore` *wird eine weitere Befehlsebene aufgerufen. Geben Sie anschließend* `restore database` *ein.*

7. *In dem darauf folgenden Sicherheitsabfragefenster klicken Sie auf OK, um die Versionsnummer der Datenbank bzw. der Datenbankobjekte automatisch um 100 000 zu erhöhen.*

8. *Nach Abschluss des Vorgangs wird der Status angezeigt (siehe Abbildung).*

9. *Geben Sie anschließend* `quit` *ein, um die Befehlsebene zu verlassen. Geben Sie erneut* `quit` *ein, um das Programm ntdsutil zu beenden.*

10. *Starten Sie den Domänencontroller neu. Über die Replikation werden nun die weiteren in der Domäne befindlichen Domänencontroller aktualisiert.*



Autorisierende Wiederherstellung

Über die Befehlsebene *authoritative restore* können auch einzelne Objekte in die Active Directory-Datenbank integriert werden. Geben Sie auf der Befehlsebene von *authoritative restore* Folgendes ein, um beispielsweise eine gelöschte Organisationseinheit mit dem Namen Personalabteilung in der Domäne Kiel.de wiederherzustellen:

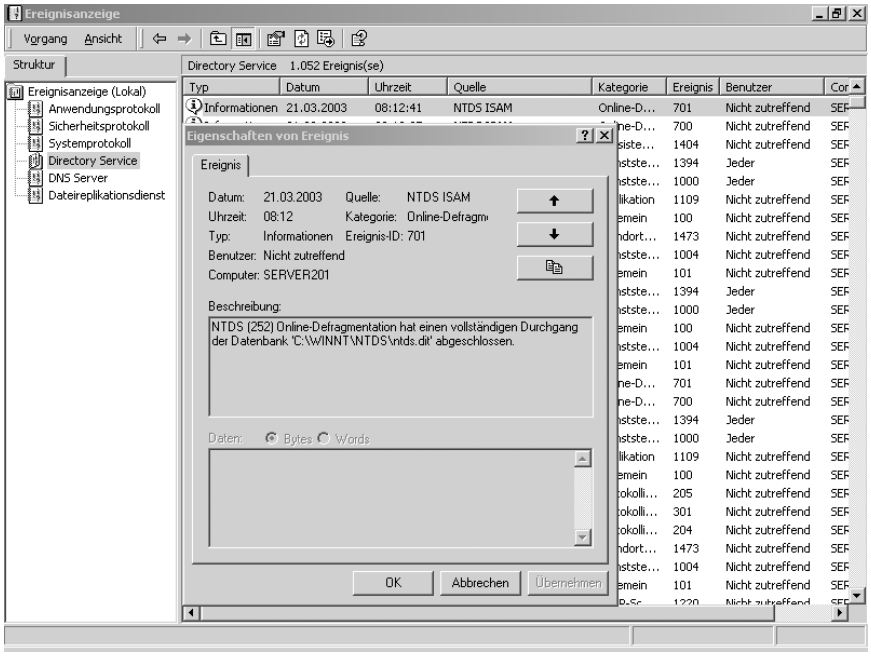
```
restore subtree OU=Personalabteilung,DC=Kiel,DC=de
```

12.3.5 Defragmentieren der Active Directory-Datenbank

Im Laufe des Betriebes wird die Active Directory-Datenbank durch die Aufnahme und Änderung von Objekten fragmentiert auf der Festplatte gespeichert. Das führt zu einer Verschlechterung der Zugriffszeiten auf Datenbankobjekte. Durch eine Defragmentierung wird die Active Directory-Datenbank in zusammenhängende „Bereiche“ neu strukturiert. Dadurch werden alle Datenbankoperationen beschleunigt. Die Defragmentierung wird online automatisch und offline manuell durchgeführt.

- **Online-Defragmentierung**

  Die Online-Defragmentierung ordnet die Objekte innerhalb der Active Directory-Datenbank standardmäßig alle 12 Stunden neu. Physikalisch behält die Datenbank auf der Festplatte jedoch die gleiche Struktur. Der Vorgang wird im Ereignisprotokoll unter Directory Service protokolliert.

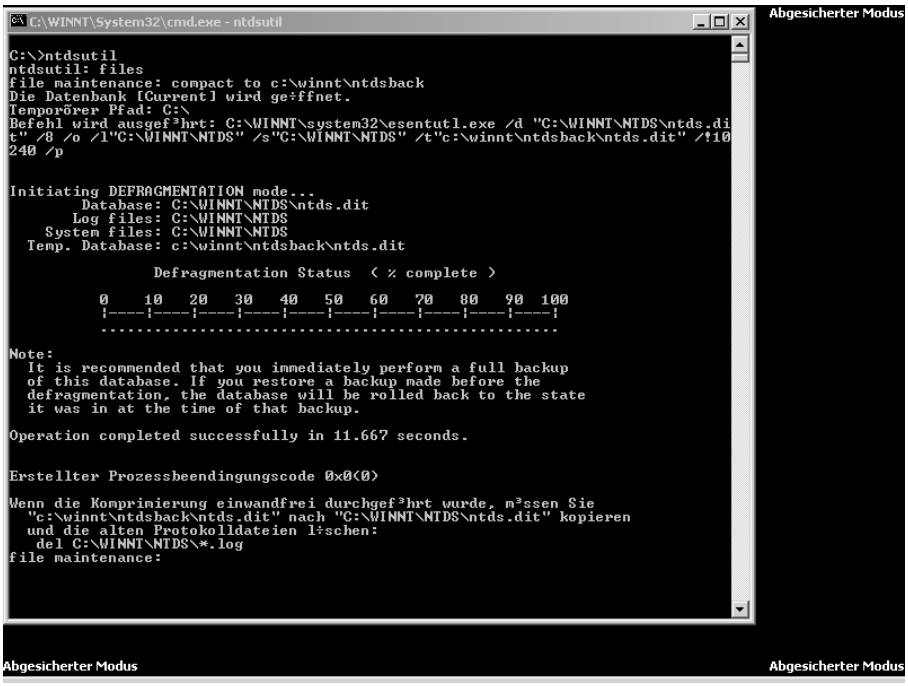


Ereignisprotokoll – Directory Service – Online-Defragmentierung

- **Offline-Defragmentierung**

  Die Offline-Defragmentierung erstellt auf der Festplatte in einem vorgegebenen Ordner eine physikalisch zusammenhängende **zweite** Datenbankdatei ntds.dit. Die fragmentierte Datenbank verbleibt zunächst noch am gleichen Ort. Durch das Neuanlegen der Daten-

bank verringert sich in der Regel die Kapazität der Datenbank. Das hängt mit den gelöschten Objekten zusammen, die in der Datenbank ursprünglich verwaltet wurden.



Programm ntdsutil – Offline-Defragmentierung

Active Directory-Datenbank offline defragmentieren!

1. *Sichern Sie als Vorsichtsmaßnahme die Active Directory-Datenbank.*
2. *Starten Sie den Domänencontroller und wechseln Sie über die Funktionstaste F8 in die erweiterten Startoptionen.*
3. *Wählen Sie die Option VERZEICHNISDIENSTWIEDERHERSTELLUNG.*
4. *Melden Sie sich unter dem Administratorkonto an.*
5. *Richten Sie einen neuen Speicherort bzw. Ordner für die Datenbank ein, z. B. mit dem Befehl* `md c:\winnt\ndtsback`.
6. *Starten Sie über die Eingabeaufforderung das Programm ntdsutil und geben Sie* `files` *ein, um die Befehlsebene FILE MAINTENANCE zu aktivieren.*
7. *Geben Sie anschließend den Befehl* `compact to c:\winnt\ndtsback` *(in diesem Beispiel) ein. Danach wird eine neue Datenbank mit dem gleichen Namen ntds.dit erstellt.*
8. *Verlassen Sie das Programm ntdsutil, indem Sie auf der Befehlsebene* `quit` *und danach nochmals* `quit` *eingeben.*

9. *Kopieren Sie (in diesem Beispiel) die neue Datenbank ntds.dit mit dem Befehl* `copy c:\winnt\ntdsback\ntds.dit c:\winnt\ndts` *über die alte Datenbankdatei.*

10. *Löschen Sie mit dem Befehl* `del C:\winnt\ntds\*.log` *die Protokolldateien.*

11. *Starten Sie danach den Domänencontroller neu.*

12.4 Sicherheitscheck

- *Erstellen Sie ein **Konzept** zur Durchführung der Datensicherung.*
- *Sichern Sie wochentags die Daten aller Server jeweils getrennt auf einem entsprechenden Datenträger mit der Sicherungsmethode **Normale Sicherung**.*
- *Berücksichtigen Sie bei der Datensicherung grundsätzlich die **Systemstatusdateien**.*
- *Erstellen Sie eine **Notfalldiskette** mit dem Windows Backup-Sicherungsprogramm. Sichern Sie dabei auch die Registrierung.*
- *Führen Sie eine **Dokumentation**, anhand derer nachvollzogen werden kann, welcher Mitarbeiter wann mit welchem Datenträger eine Datensicherung durchgeführt hat.*
- *Hinterlegen Sie eine **Wochensicherung** in einem verschließbaren Behältnis außerhalb Ihrer Organisation.*
- *Führen Sie zu **Testzwecken** regelmäßig Wiederherstellungen durch.*
- *Installieren Sie auf den Servern die **Wiederherstellungskonsole** von der Windows 2000-Installations-CD.*
- *Sofern das Betriebssystem nicht mehr **fehlerfrei** funktioniert, benutzen Sie erst die Notfallreparaturkonsole. Werden die Fehler über die Notfallreparaturkonsole nicht behoben, setzen Sie die Wiederherstellungskonsole ein.*
- *Ist die Active Directory-Datenbank **beschädigt**, führen Sie vor einer Rücksicherung der Datenbank von einem Datenträger im Verzeichnisdienstwiederherstellungsmodus das Programm ntdsutil aus. Über die Befehle **recover** und **repair** kann die Datenbank repariert werden.*
- *Ist eine Reparatur nicht möglich, führen Sie die Wiederherstellung der Active Directory-Datenbank über einen **Datenträger** der Datensicherung durch.*
- *Führen Sie in regelmäßigen Zeitabständen, z. B. zweimal im Jahr, eine **Offline-Defragmentierung** der Active Directory-Datenbank durch.*

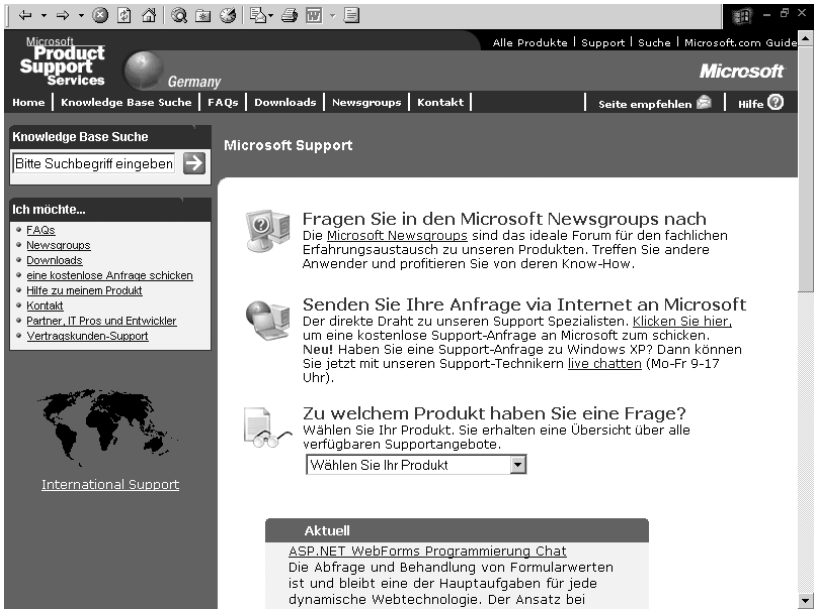
13 Hilfreiche Internetwebseiten

In diesem Kapitel werden einige Webseiten dargestellt, die Ihnen

- bei administrativen Problemen weiterhelfen können,
- Security-Tools für die Administration von Windows 2000 aufzeigen und
- allgemeine Informationen zur Datensicherheit präsentieren.

13.1 Microsoft.com

Die Microsoft-Webseiten bieten ein breites Angebot an Informationen. Besonders hilfreich ist die Supportseite, über die z. B. die Knowledge Base oder die Downloadseite mit Updates und Service Packs aufgerufen werden kann.



http://support.microsoft.com/

Die Knowledge Base ist eine umfassende Online-Datenbank mit technischen Artikeln sowohl in Deutsch als auch in Englisch. Durch die Eingabe von Stichwörtern kann gezielt nach Informationen gesucht werden. Die Knowledge Base enthält momentan ca. 17000 deutschsprachige und über 100000 englischsprachige Artikel. Viele Artikel beinhalten darüber hinaus auch eine Schrittanleitung zur Konfiguration des Systems.

Die Webseite Security informiert hingegen über Schutzmöglichkeiten in den Bereichen Prozesse und Technologien, Desktop-Sicherheit und Server- und Applikationssicherheit. Beschreibungen erfolgreicher Strategien und Projekte wie auch technische Anweisungen und Whitepapers geben verständliche Antworten auf Fragen zur Sicherheit.

http://www.microsoft.com/germany/ms/security/

13.2 NThelp.de

http://www.nthelp.de

Auf der Seite *nthelp* werden insbesondere nützliche Informationen für Administratoren bereitgestellt. Die Seite verfügt darüber hinaus über viele interessante Links. Besonders erwähnenswert sind die IT-Diskussionsforen. Diese werden von Insidern intensiv genutzt, sodass man in diesem Bereich für technische Probleme schnell Lösungen findet.

13.3 WebAttack.com

http://www.webattack.com

WebAttack ist keine Hackerseite, sondern ein Verzeichnis über Software-Tools. Es werden zahlreiche Tools als Free- oder Shareware angeboten. Darunter befinden sich auch viele Security-Tools. Der Funktionsumfang der Tools wird kurz beschrieben. Die Software kann sofort heruntergeladen und eingesetzt werden.

13.4 NTSecurity.nu

Auf dieser Webseite können u. a. nützliche Security-Tools als Freeware heruntergeladen werden. Des Weiteren finden sich auf der Homepage viele Links zu Hacker- und Security-Webseiten.

http://www.ntsecurity.nu/toolbox/

13.5 Protect-me.com

http://www.protect-me.com/dl/index.htm

Mit dem Security-Tool *DeviceLock* können Disketten-, CD-ROM-Laufwerke, serielle und parallele Ports, zusätzliche Festplatten sowie Speichererweiterungen, wie z. B. USB-Sticks, benutzerbezogen verwaltet werden. Das Tool kann über das Netzwerk installiert werden.

13.6 SystemTools.com

Die Webseite *SystemTools* enthält u. a. zahlreiche Freeware-Programme. Für die Kontrolle und Dokumentation der NTFS-Rechte ist *DumpSec* zu empfehlen. Dieses Tool kann als Freeware heruntergeladen und sollte zur Unterstützung der Administration eingesetzt werden.

http://www.systemtools.com

13.7 Datenschutzzentrum.de

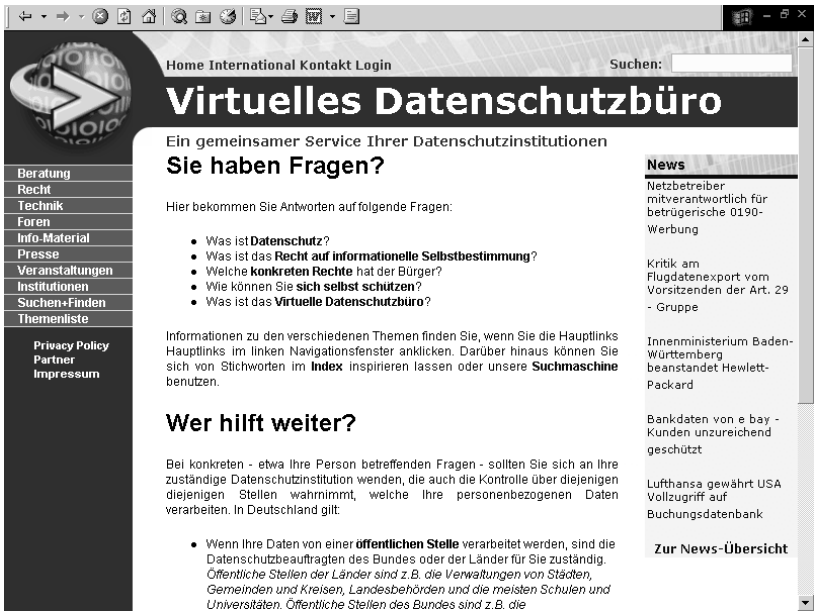
Auf der Webseite des Unabhängigen Landeszentrums für Datenschutz können vielfältige Informationen zum Datenschutz und zur Datensicherheit abgerufen werden. Dazu zählen auch alle bisher erschienenen *backUP*-Magazine, die als PDF-Dateien zum Download bereit stehen.

Unter <www.datenschutzzentrum.de/systemdatenschutz> findet sich unser neuer Informationsdienst für Systemadministratoren mit

- Kommentaren zu aktuellen Problemen der Datensicherheit,
- Rezensionen von Artikeln, Broschüren und Büchern zur Datensicherheit und
- Veranstaltungsankündigungen im Bereich IT-Sicherheit und Systemdatenschutz.

http://www.datenschutzzentrum.de

13.8 Datenschutz.de



http://www.datenschutz.de/beratung/

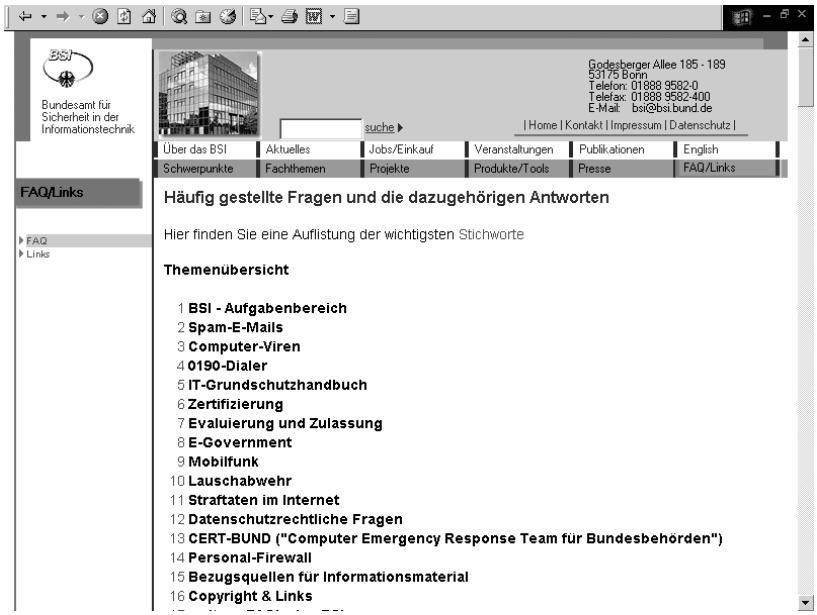
Das virtuelle Datenschutzbüro ist ein Portal zum Datenschutz. Eine große Anzahl von Beiträgen und Artikeln kann aufgerufen werden, und viele Links verweisen auf weiter gehende Informationen im Internet.

13.9 IT-Audit.de

Die Webseite *IT-Audit* legt neben der IT-Sicherheit einen Schwerpunkt auf die IT-Revision. Datenschutzbeauftragte und IT-Revisoren finden auf dieser Seite Gesetze und Verordnungen sowie nützliche Hinweise für die tägliche Arbeit. Veröffentlichungen zum Datenschutz und zur Datensicherheit können per Download heruntergeladen werden.

http://www.it-audit.de

13.10 BSI.de

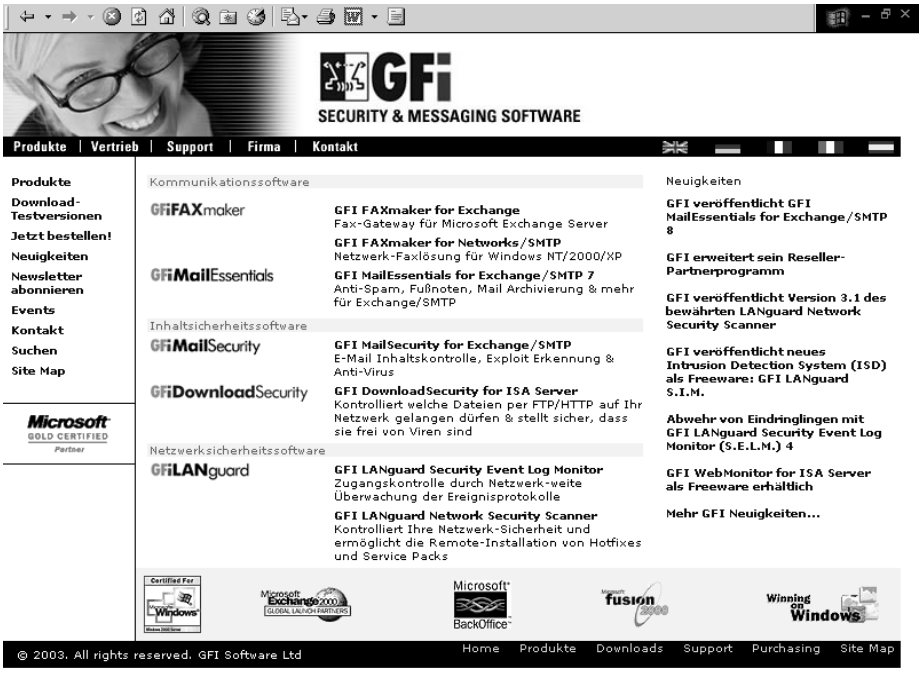


http://www.bsi.de

Die Seite des *BSI* bietet zahlreiche Informationen zur Datensicherheit. Vielseitige Fachthemen, Produktinformationen, Virenmeldungen, Publikationen und Veranstaltungshinweise können abgefragt werden.

13.11 GFISoftware.de

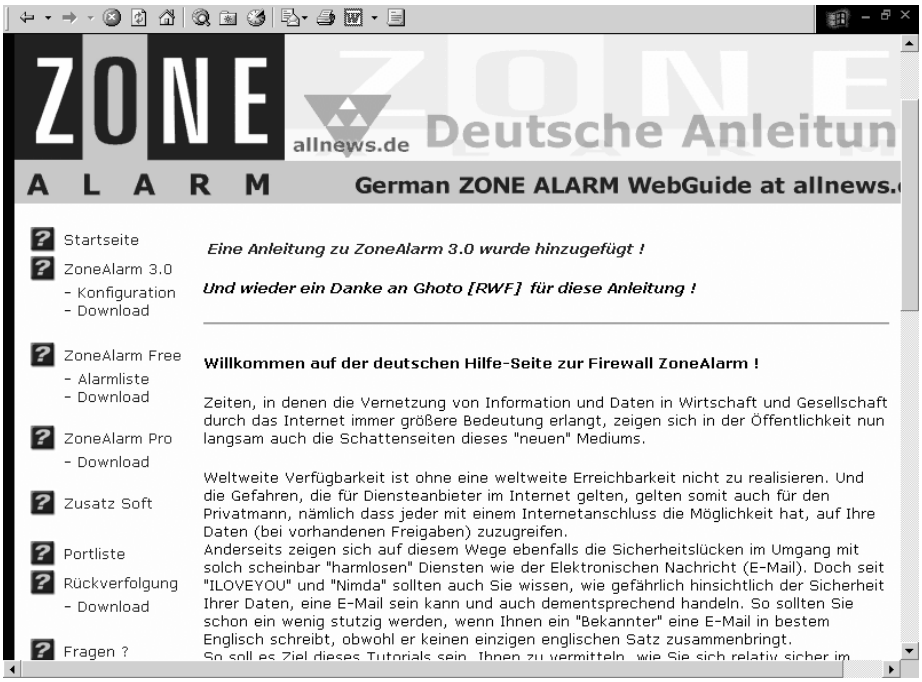
GFI ist ein führender Anbieter von Produkten für Content- und Netzwerk-Sicherheit, die auf Windows NT/2000/XP basieren. Die meisten Software-Lösungen können als Testversion heruntergeladen werden. Dazu gehört auch der Security-Scanner „LANGuard“.



http://www.gfisoftware.de/

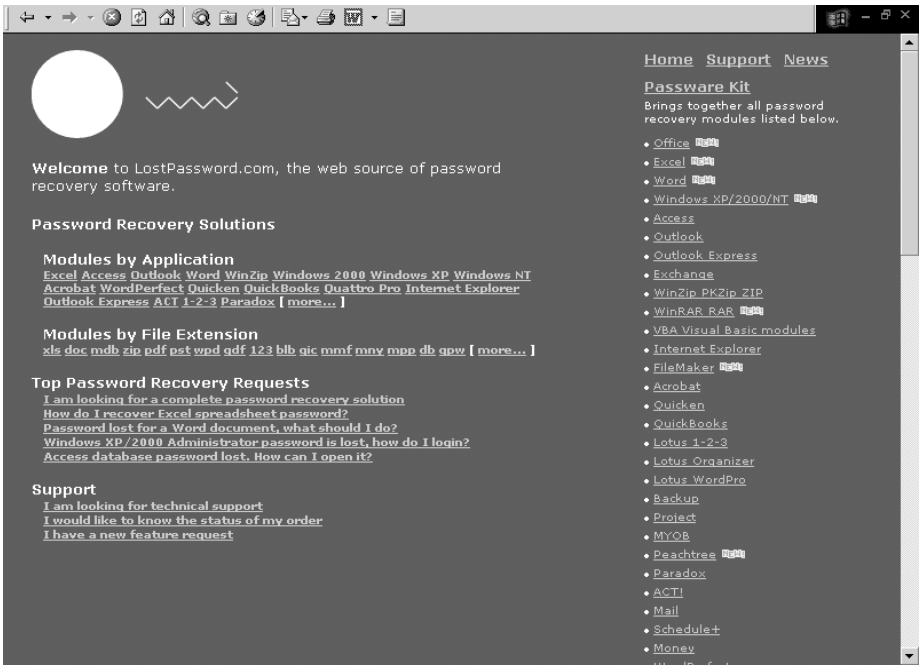
13.12 Zonealarm.de

Zonealarm ist eine geeignete Firewallsoftware für einzelne Computer, die an das Internet angeschlossen sind. Die Firewall filtert die Datenkommunikation und verhindert unerwünschte Zugriffe (z. B. einen Portscan) auf den PC.



http://www.zonealarm.de/

13.13 LostPassword.com



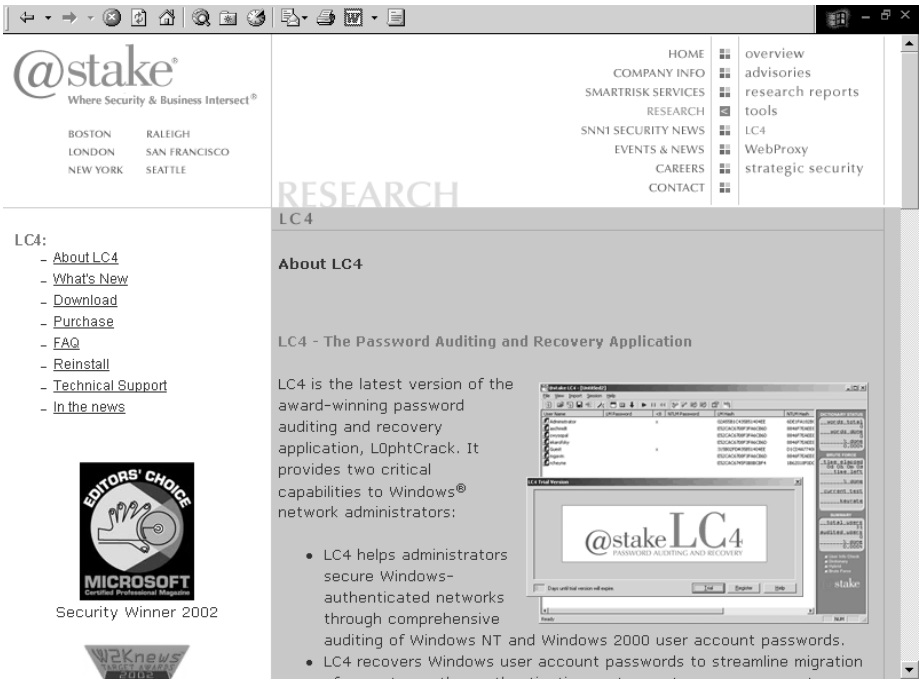
http://www.lostpassword.com/

Diese Webseite bietet für die gängigsten Produkte Password-Recovery-Tools an. Mithilfe dieser Tools können vergebene bzw. vergessene Passwörter offen gelegt werden. Dazu gehö-

ren z. B. die Word-Kennwörter oder das Kennwort des Domänenadministrators unter Windows 2000.

13.14 Atstake.com

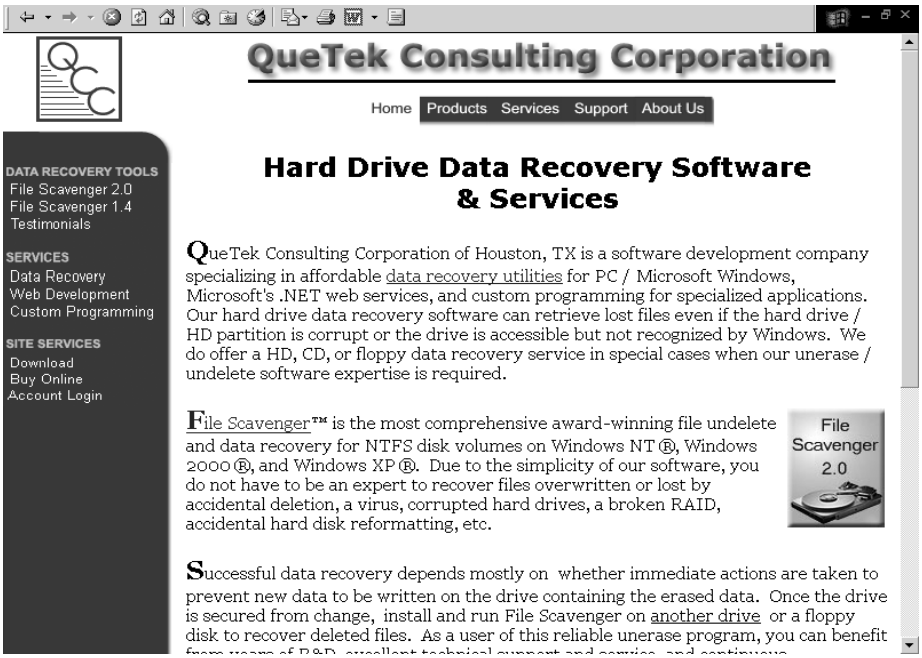
Von der Webseite *atstake* kann das Programm *L0phtcrack* heruntergeladen werden. L0phtcrack ist in der Lage, die unter Windows NT/2000 verwalteten Benutzerkonten auszulesen und die vergebenen Kennwörter zu knacken. Die neueste für Windows 2000 angebotene Version LC4 ist nach dem Download kostenlos nur eingeschränkt nutzbar. Die Version 2.5 für Windows NT enthält keine Einschränkung, ist jedoch in der Nutzung auf 15 Tage begrenzt.



http://www.atstake.com

13.15 QueTek.com

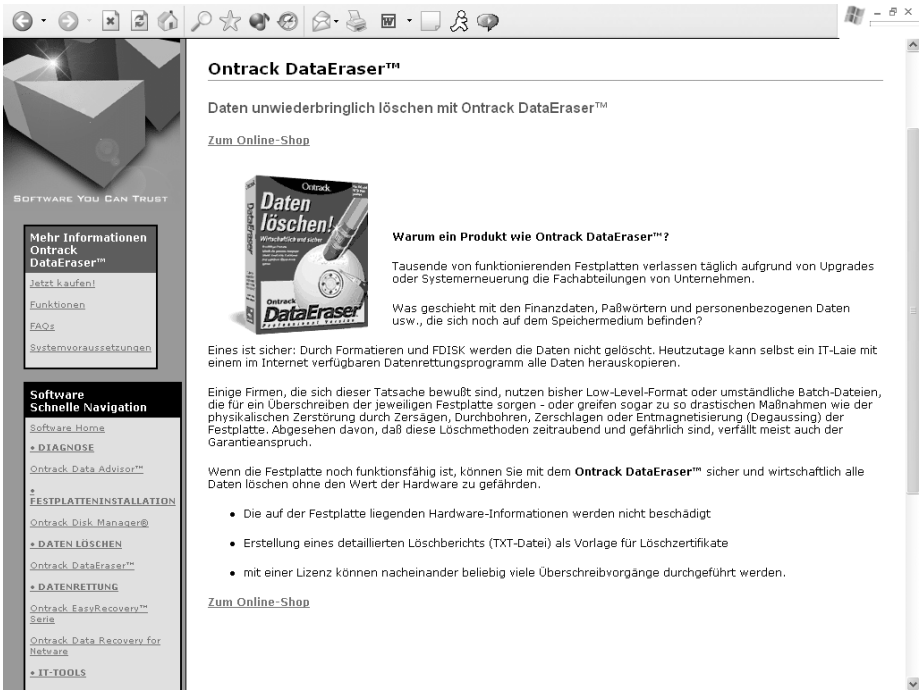
Diese Webseite macht deutlich, dass auf der Festplatte gelöschte Dateien tatsächlich noch vorhanden sind.



http://www.quetek.com

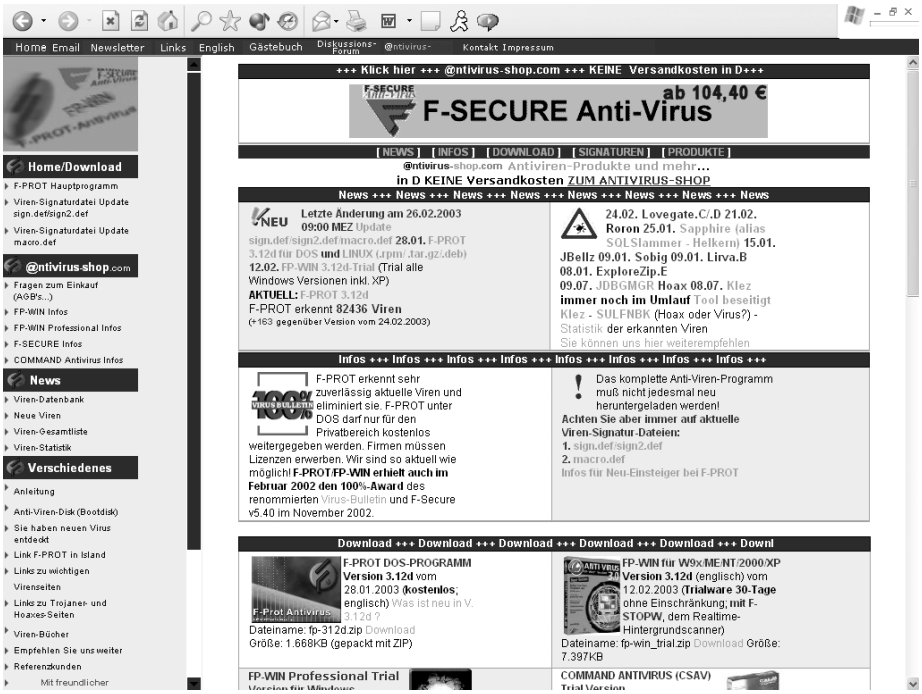
13.16 Ontrack.de

Durch den Einsatz dieses Tools kann gewährleistet werden, dass die gelöschten Daten auf der Festplatte auch tatsächlich nicht mehr rekonstruierbar sind.



http://www.ontrack.de/dataeraser/

13.17 Fprot.org



http://www.fprot.org/

Die Webseite *fprot* enthält Informationen über den Virenschutz. Es wird über aktuelle im Umlauf befindliche Viren berichtet und Anti-Virus-Programme zum Herunterladen angeboten. Die Seite verfügt über eine Virendatenbank, in der die meisten Viren beschrieben werden, und gibt dem Benutzer nützliche Tipps bei der Bekämpfung einer Vireninfizierung.

14 Checkliste Windows 2000

In diesem Kapitel werden zwei Checklisten dargestellt, die

- Ihnen bei der Umsetzung technischer und organisatorischer Sicherheitsmaßnahmen behilflich sein können und
- Ihnen für die Kontrolle bereits durchgeführter Sicherheitsmaßnahmen dienen.

14.1 Technische Sicherheitsmaßnahmen

14.1.1 Implementierung

Komponenten	Installieren Sie nur die Betriebssystemkomponenten, die benötigt werden.
Dateisystem	Richten Sie das Dateisystem NTFS (New Technology File System) bereits während der Installation ein. Das Dateisystem FAT enthält keine Dateiberechtigungen.
Service Pack	Installieren Sie nach der Installation von Windows 2000 das aktuelle Service Pack. (Achtung: Nach jeder Installation von Software müssen Sie das Service Pack erneut installieren)
Bootvorgang	Nehmen Sie in der Datei boot.ini folgende Einstellung vor: timeout=0.
Repairordner	In dem Ordner <Stammverzeichnis:\winnt\repair\> befinden sich „sensible“ Konfigurationsdaten, wie z. B. die Benutzer- und Passwortdaten (SAM-Datei). Standardmäßig hat die Gruppe „Authentifizierte Benutzer“ lesenden Zugriff. Entfernen Sie diese Gruppe aus den SICHERHEITSEINSTELLUNGEN (rechter Mausklick auf den Ordner *repair*).
Defragmentierung	Installieren Sie ein Defragmentierungsprogramm (z. B. www.sysinternals.com), um die Verfügbarkeit der Systemdateien (Registrydatenbank und pagefile.sys) zu erhöhen. Stellen Sie die Dateien auf eine konstant ausreichende Kapazität ein.

Support-Tools	Installieren Sie die Support-Tools.
Adminpak	Installieren Sie die zusätzlichen Verwaltungsprogramme aus dem *Adminpak*.
Clientlaufwerke	Setzen Sie ein Tool für die Verwaltung und Deaktivierung der Disketten- und CD-ROM-Laufwerke sowie für Schnittsellen (USB-Port) ein (z. B. DeviceLock).

14.1.2 Active Directory, Benutzer- und Gruppenverwaltung

Organisationseinheiten	Legen Sie analog zum Geschäftsverteilungsplan für die einzelnen Fachabteilungen Organisationseinheiten an. Nehmen Sie in den entsprechenden Organisationseinheiten die Benutzer- und Gruppenkonten auf.
Globale Gruppen	Legen Sie globale Gruppenkonten für Benutzer mit gleichen Aufgaben an. Wählen Sie grundsätzlich den Gruppentyp Sicherheit.
Lokale Gruppen	Legen Sie lokale Gruppenkonten für die Fachanwendungen an.
Standardgruppe Domänen-Admins und Administratoren	Fügen Sie nur die Benutzerkonten in die Gruppen *Domänen-Admins* und *Administratoren* ein, die volle Administrationsrechte erhalten sollen. Das Gleiche gilt für die Gruppen *Schema-Admins* und *Organisations-Admins.*
Sonstige Admin-Standardgruppen	Ordnen Sie für spezielle administrative Aufgaben die Benutzer den Standardgruppen (*Kontenoperatoren, Sicherungsoperatoren* usw.) zu, legen Sie ggf. spezielle Admin-Gruppen an.
Administrator	Verwenden Sie dieses Konto nicht für administrative Zwecke. Wählen Sie ein sicheres Kennwort und ändern Sie es regelmäßig.
Admin-Konto für externe Dienstleister	Richten Sie für externe Dienstleister ein separates Konto ein. Deaktivieren Sie dieses Konto standardmäßig.
Admin-Konto	Richten Sie für jeden Administrator ein gesondertes Konto ein.

Gast	Deaktivieren Sie das Gastkonto.
Mitarbeiterkonten	Richten Sie die Konten unter Angabe der Funktion oder der Zuordnung der Abteilung innerhalb der Organisationseinheiten ein. Löschen Sie die Konten von Mitarbeitern, die die Organisation verlassen haben.
Benutzerkonten auf den Clients	Richten Sie auf den Clients keine lokalen Benutzerkonten ein. Die Anmeldung erfolgt grundsätzlich nur an der Domäne.
Schalter: BENUTZER MUSS KENNWORT BEI DER NÄCHSTEN ANMELDUNG ÄNDERN	Aktivieren Sie für neu erstellte Konten diesen Schalter.
Schalter: KENNWORT LÄUFT NIE AB	Deaktivieren Sie bei Mitarbeiterkonten diesen Schalter grundsätzlich.
Schalter: KONTO DEAKTIVIERT	Aktivieren Sie diesen Schalter, wenn ein Mitarbeiter die Organisation vorübergehend (z. B. Erziehungsurlaub) verlassen hat.
Anmeldezeiten	Legen Sie je nach Benutzeranforderungen und Sicherheitsrichtlinien die Anmeldezeiten fest.
Anmelden an	Begrenzen Sie je nach organisatorischen Verhältnissen die Anmeldung auf wenige PC. Geben Sie den bzw. die Computernamen ein.
Ablaufdatum des Kontos	Tragen Sie ein Ablaufdatum ein, bei dessen Erreichen das Benutzerkonto automatisch gesperrt werden soll, z. B. bei befristet eingestellten Mitarbeitern.
Einwählen (RAS)	Vergeben Sie diese Berechtigung nur an Benutzer, die über einen Remote-Zugriff (Einwahl von extern) verfügen. Die Option RÜCKRUFOPTIONEN ist unter Angabe der Rückrufnummer zu aktivieren.

14.1.3 Gruppenrichtlinie (Default Domain Policy)

Computerkonfiguration/Sicherheitseinstellungen/Kontorichtlinien/Kennwortrichtlinien	
Richtlinien	**Einstellung**
Kennwortchronik erzwingen	10 Kennwörter aufbewahren
Kennwörter müssen den Komplexitätsanforderungen entsprechen	Schalter aktivieren, um komplexe Kennwörter zu erzwingen
Kennwörter für alle Domänenbenutzer mit umkehrbarer Verschlüsselung speichern	Schalter nicht aktivieren, da sonst die Kennwort mit einer schwachen Verschlüsselung verschlüsselt werden
Maximales Kennwortalter (Tage)	30-90 Tage
Minimale Kennwortlänge	7 Zeichen
Minimales Kennwortalter	erste Änderung nach 3 Tagen erlauben, um zu verhindern, dass ein altes Kennwort wieder gewählt wird

Computerkonfiguration/Sicherheitseinstellungen/Kontorichtlinien/Kontosperrungsrichtlinien	
Richtlinien	**Einstellung**
Kontosperrungsschwelle	3 ungültige Kennworteingaben
Kontosperrdauer	0 Minuten (bis der Administrator sie aufhebt und die Ursache für die Fehleingaben aufgeklärt hat)
Kontosperrungszähler zurücksetzen nach	30 Minuten, d. h., die Anzahl von Fehleingaben wird nach 30 Minuten wieder auf null gesetzt

Computerkonfiguration/Sicherheitseinstellungen/Lokale Richtlinien/Überwachungsrichtlinien	
Richtlinie	**Einstellung**
Anmeldeversuche überwachen	Fehlgeschlagen: Fehlerhafte Anmeldeversuche am Client werden im Sicherheitsprotokoll des Clients protokolliert.

14.1.4 Gruppenrichtlinie (Default Domain Controllers Policy)

Computerkonfiguration/Sicherheitseinstellungen/Lokale Richtlinien/Überwachungsrichtlinien	
Richtlinie	**Einstellung**
Anmeldeversuche überwachen	Fehlgeschlagen: Konsole des Domänencontrollers wird bezüglich fehlerhafter Anmeldungen überwacht.
Kontenverwaltung überwachen	Erfolgreich, Fehlgeschlagen: Administrative Veränderungen der Benutzer- und Gruppenkonten werden protokolliert.
Objektzugriffsversuche überwachen	Erfolgreich: Es müssen Ordner oder Dateien zusätzlich bestimmt werden, die in Bezug auf einen Zugriff durch Administratoren oder Benutzer überwacht werden sollen.
Richtlinienänderung überwachen	Erfolgreich, Fehlgeschlagen: Administrative Veränderungen der *Lokalen Richtlinien* werden protokolliert.

14.1.5 Gruppenrichtlinie für Organisationseinheiten

Benutzerkonfiguration/Windows-Komponenten/Administrative Vorlagen/Windows Explorer	
Richtlinie	**Einstellung**
Menü *Datei* aus *Windows Explorer* entfernen	entfernt das Menü *Datei* aus dem *Windows Explorer*

Optionen *Netzwerklaufwerk verbinden* und *Netzwerklaufwerk trennen* entfernen	entfernt Menüeinträge *Netzlaufwerk verbinden* und *Netzlaufwerk trennen* von der Symbolleiste und aus den Menüs *Extras* im *Windows Explorer* und in der *Netzwerkumgebung*
Standardkontextmenü des Windows Explorers deaktivieren	entfernt Kontextmenüs vom Desktop und aus dem Windows Explorer
Diese angegebenen Datenträger im Fenster *Arbeitsplatz* entfernen	entfernt die Symbole für ausgewählte Laufwerke aus *Arbeitsplatz*, *Windows Explorer* und *Netzwerkumgebung*
Symbol *Gesamtes Netzwerk* nicht in *Netzwerkumgebung* anzeigen	deaktiviert *Netzwerkumgebung* im *Windows Explorer*

Benutzerkonfiguration/Administrative Vorlagen/Startmenü und Taskleiste	
Richtlinie	**Einstellung**
Verknüpfungen für Windows Update deaktivieren und entfernen	deaktiviert die Windows Update-Funktion
Standardprogrammgruppen aus dem Startmenü entfernen	zeigt nur die Objekte aus dem Profil des Benutzers im Menü *Programme* an
Programme im Menü *Einstellungen* deaktivieren	entfernt *Systemsteuerung*, *Drucker*, *Netzwerk- und DFÜ-Verbindungen* aus dem *Startmenü*, aus *Arbeitsplatz* und *Windows Explorer*
Menüeintrag *Netzwerk- und DFÜ-Verbindungen* aus dem Startmenü entfernen	entfernt den Ordner *Netzwerk- und DFÜ-Verbindungen*
Menüeintrag *Hilfe* aus dem	entfernt den Menüeintrag *Hilfe* aus dem *Startmenü*

Startmenü entfernen	
Menüeintrag *Ausführen* aus dem Startmenü entfernen	entfernt den Menüeintrag *Ausführen* aus dem *Startmenü* und den Befehl *Neuer Task (Ausführen)* im *Task-Manager*
Ändern der Einstellungen für die Taskleiste und das Startmenü nicht zulassen	entfernt den Menüeintrag *Taskleiste und Startmenü* aus dem Menü *Einstellungen* im *Startmenü*
Kontextmenü der Taskleiste deaktivieren	blendet die Menüs, die mit einem Rechtsklick auf die Taskleiste angezeigt werden, aus

Benutzerkonfiguration/Administrative Vorlagen/Desktop	
Richtlinie	**Einstellung**
Symbol *Eigene Dateien* vom Desktop entfernen	entfernt das Symbol *Eigene Dateien* vom *Desktop*, aus *Windows Explorer*, aus Programmen, die Windows Explorer-Fenster verwenden, und aus dem Standarddialog *Öffnen*
Desktop-Symbol *Netzwerkumgebung* ausblenden	entfernt das Symbol *Netzwerkumgebung* vom Desktop
Internet Explorer-Symbol auf dem Desktop ausblenden	entfernt das Symbol *Internet Explorer* vom Desktop und von der Schnellstartleiste auf der Taskleiste

14.1.6 Datenverwaltung

Workstation	Löschen Sie auf der Workstation alle unnötigen Ordner.
Server	Legen Sie auf dem Server Ordner für die Fachanwendungen an. Erzeugen Sie für Standardsoftware (z. B. Word, Excel) eine Dokumentenablage (angelehnt an den Geschäftsverteilungsplan) für jeden Benutzer. Integrieren Sie den zentralen Schreibdienst mit einem Ordner in die Ab-

	lagestruktur der Fachbereiche. Vergeben Sie die Zugriffsrechte unter Berücksichtigung einer fachbereichsbezogenen Datenabschottung. Schützen Sie sensible Daten innerhalb der Dokumentenablage auch vor Zugriffen der Administration.

14.1.7 Zugriffsrechte und Berechtigungen

Freigaben	Freigabeberechtigungen, die der Benutzer nicht sehen soll, sollten Sie durch Eingabe eines Dollarzeichens ($) als letztes Zeichen im Freigabenamen unsichtbar machen.
die Gruppe *Jeder*	Bei der Zuweisung von Freigaben wird automatisch die Gruppe *Jeder* systemseitig eingetragen. Sofern kein allgemeiner Zugriff erforderlich ist, tragen Sie nur befugte Benutzerkonten ein.
Aufruf der freigegebenen Ressourcen	Integrieren Sie die freigegebenen Ressourcen ggf. in die Bedieneroberfläche der entsprechenden Benutzer, sodass sie nicht über den Explorer auf die Ressource zugreifen müssen (z. B. Drucker, Anwendungen, Datenablage).
NTFS-Benutzerkontenrechte auf dem Client	Setzen Sie auf dem Client NTFS-Zugriffsrechte, sodass in den Ordnern keine Datenbestände abgelegt werden können (soweit möglich).
NTFS-Benutzerkontenrechte auf dem Server	Vergeben Sie auf dem Server (soweit möglich) Gruppenkonten NTFS-Zugriffsrechte. Gewährleisten Sie eine fachbereichsbezogene Datenabschottung.
Freigabe- und NTFS-Berechtigungen kombinieren	Kombinieren Sie die Vergabe von Freigabe- und NTFS-Zugriffsrechten.
Zugriff Administratoren	Sie sollten den Administratoren die Zugriffsrechte auf die Dokumentenablage so weit wie möglich entziehen. Mit der Besitzübernahme durch

	den Benutzer eines Ordners ist eine Revision des Datenbestandes auf dem Server möglich.
Benutzer	Vergeben Sie Benutzern für die Dokumentenablage (mit Ausnahme ihres eigenen Ordners) keine Rechte für die Änderung von Zugriffsrechten. Sie dürfen ausschließlich nur auf die Ordner/Dateien zugreifen, die für die Erledigung ihrer Aufgaben notwendig sind.
Rechtevergabe prüfen	Prüfen Sie die an Benutzerkonten vergebenen Zugriffsrechte über das entsprechende Benutzerkonto. Setzen Sie zur Überprüfung von NTFS-Berechtigungen ein Hilfstool ein. Kontrollieren Sie die Berechtigungen über das Tool in regelmäßigen Abständen.

14.1.8 Benutzerprofile und Basisordner

Anlegen von servergespeicherten Profilen	Legen Sie servergespeicherte Profile auf dem Server in einem gesonderten Verzeichnis/Ordner an.
Versteckte Freigabe	Richten Sie diesen Ordner mit einer versteckten Freigabe ein.
Benutzerkonten	Geben Sie in den Benutzerkonten den entsprechenden Server-Pfad an.
Basisordner	Geben Sie für jedes Benutzerkonto einen Basisordner an, der in der Dokumentenablage integriert wird.
Pfadangabe für Speicherort	Geben Sie in den Einstellungen der Standardsoftware (Word, Excel) den Pfad des Basisordners an.

14.1.9 Überwachung

Revisor	Legen Sie für die Überwachung und Auswertung der erzeugten Protokolle ein Revisor-Benutzerkonto an. Schränken Sie das Benutzerkonto so ein, dass ausschließlich die *Ereignisanzeige* und ein Textverarbeitungsprogramm zur Verfügung stehen. Legen Sie zur Archivierung der Proto-

	kolle einen gesonderten Ordner auf dem Server an. Begrenzen Sie die Zugriffsrechte ausschließlich auf das Revisor-Benutzerkonto.
Protokoll Ereignisanzeige	Stellen Sie in der *Ereignisanzeige* das Sicherheitsprotokoll auf 10 MB Speicherkapazität ein. Das Protokoll sollte frühestens nach 7 Tagen überschrieben werden.

14.1.10 Dokumentation

Benutzereinstellungen	Sie sollten in der Lage sein, die Benutzer- und Gruppenkontenverwaltung sowie die Freigabe- und NTFS-Berechtigungen mithilfe von Tools revisionsfähig darzustellen.
Gruppenrichtlinien	Dokumentieren Sie die aktivierten Gruppenrichtlinien.
Sonstige Konfiguration	Setzen Sie für die Netzwerkumgebung und die Netzwerkparameter, für den Hard- und Softwarebestand sowie für die Geräteausstattung geeignete Tools ein. Nehmen Sie Konfigurationsparameter der einzelnen Bereiche in der Systemakte auf.

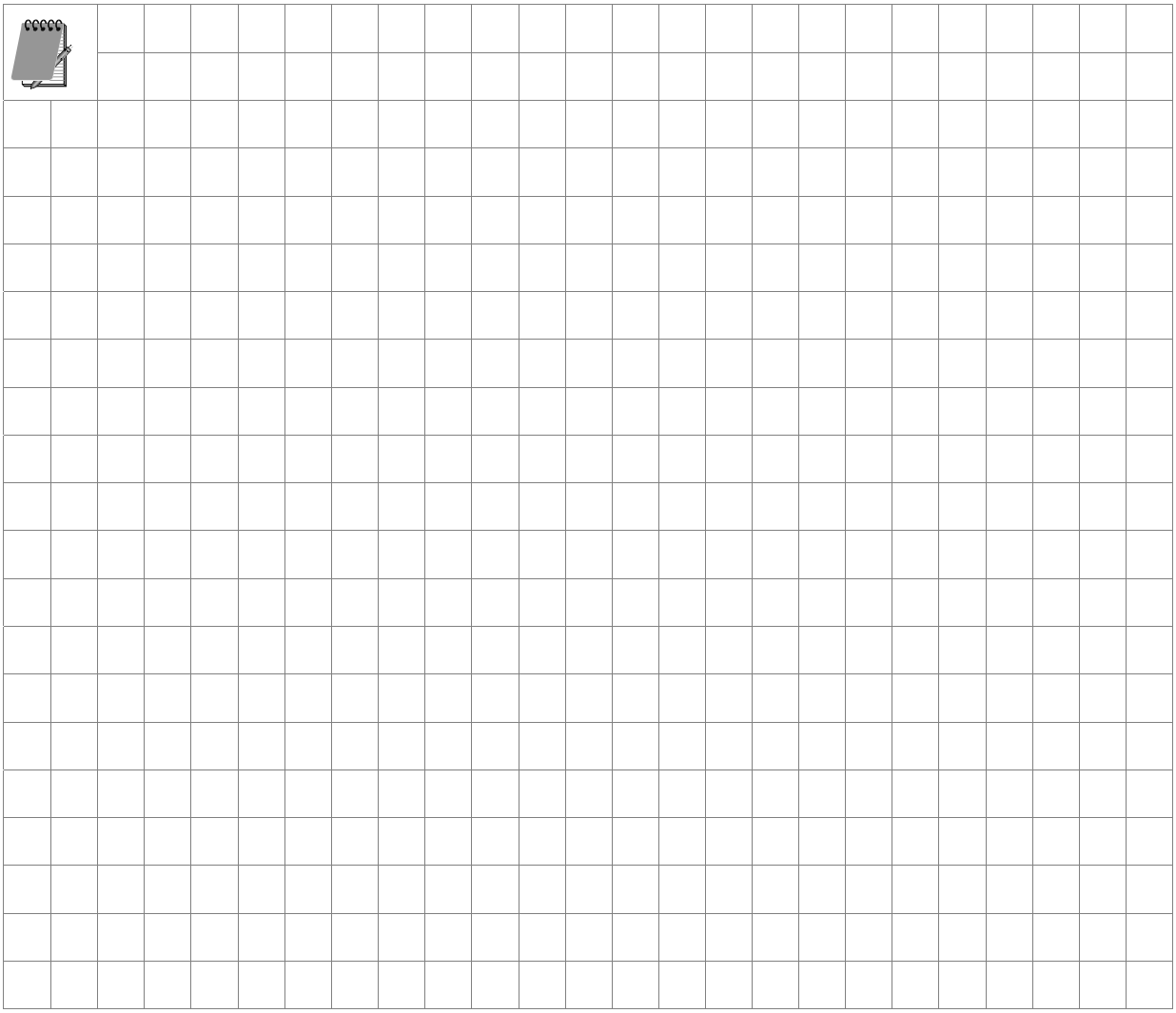
14.2 Organisatorische Sicherheitsmaßnahmen

Sicherheitsmaßnahme	**Ja**	**Nein**
Existiert ein IT-Konzept, aus dem der Hard- und Softwarebestand sowie die eingesetzten Verfahren ersichtlich sind?	☐	☐
Wurde das Sicherheitsniveau in einem Sicherheitskonzept festgelegt?	☐	☐
Werden die eingesetzten Verfahren freigegeben und revisionsfähig dokumentiert?	☐	☐
Existiert eine Dienstanweisung für die Administration der IT-Systeme?	☐	☐
Werden diese Handlungsanweisungen allen Beteiligten in geeigneter Weise bekannt gegeben?	☐	☐

Werden für die Systemaktivitäten der Administratoren Systemakten geführt?	☐	☐
Gibt es Regelungen zur Bekämpfung von Computerviren?	☐	☐
Liegt eine Netzwerkübersicht vor?	☐	☐
Bestehen Vertrauensstellungen zu anderen Domänen bzw. können externe Personen auf interne Daten zugreifen?	☐	☐
Erfolgt die Benutzerverwaltung revisionsfähig?	☐	☐
Wird die Gültigkeit der Benutzerberechtigungen regelmäßig überprüft?	☐	☐
Ist die Vergabe von Zugriffsrechten geregelt?	☐	☐
Werden Passwörter nach definierten Regeln vergeben?	☐	☐
Ist das Passwort nur dem Benutzer bekannt?	☐	☐
Sind die Mitarbeiter ausreichend geschult?	☐	☐
Erfolgt eine Absicherung der Server- und Verteilerräume?	☐	☐
Ist der Verschluss dieser Räume bei Abwesenheit angeordnet?	☐	☐
Wurde für die Durchführung der Fernwartung ein Vertrag mit dem Dienstleister geschlossen?	☐	☐
Werden die Aktivitäten der Fernwartung protokolliert und überwacht?	☐	☐
Ist das Datensicherungsverfahren schriftlich dokumentiert?	☐	☐
Sind die Verantwortlichkeiten für die Datensicherung geregelt?	☐	☐
Werden die Datenträger zugriffs- und brandsicher aufbewahrt?	☐	☐
Werden die Aktivitäten der Administratoren protokolliert und überwacht?	☐	☐
Werden Protokolldateien in regelmäßigen Abständen ausgewertet?	☐	☐
Werden die im Sicherheitskonzept festgelegten Sicherheitsmaßnahmen umgesetzt und eingehalten?	☐	☐

Ist ein Datenschutzbeauftragter bestellt worden?	☐	☐
Wird die Vorabkontrolle (LDSG) für „sensible Verfahren“ durchgeführt?	☐	☐
Wird der Datenschutzbeauftragte rechtzeitig über alle organisatorischen und technischen Maßnahmen informiert?	☐	☐
Verfügt der Datenschutzbeauftragte über alle Dokumentationsunterlagen?	☐	☐
Wird ein Verfahrensverzeichnis geführt?	☐	☐
Finden regelmäßig zwischen den IT-Verantwortlichen und den Fachbereichsverantwortlichen Besprechungen über den IT-Einsatz statt?	☐	☐
Ist festgelegt, wo welche Datenbestände gespeichert werden?	☐	☐
Wurden Löschungsregelungen für die Datenbestände der Fachbereiche festgelegt?	☐	☐
Gibt es Regelungen für die Datenverwaltung im zentralen Schreibdienst?	☐	☐
Sicherheitsmaßnahme	Ja	Nein
Liegen die Dokumente des Schreibdienstes in der Verantwortung ihrer „Auftraggeber“?	☐	☐
Ist eine fachbereichsbezogene Datenabschottung gewährleistet?	☐	☐
Bestehen Regelungen für die Nutzung der Standardsoftware Excel und Access?	☐	☐
Dürfen Mitarbeiter umfangreiche Anwendungen in Excel und/oder Access programmieren?	☐	☐
Werden die Leitungsebene und die IT-Verantwortlichen bei der Programmierung von Excel- und Access-Anwendungen durch die Mitarbeiter mit einbezogen?	☐	☐
Besteht für die Internetkommunikation ein Anforderungsprofil?	☐	☐
Wurde für den Internetanschluss ein Sicherheitskonzept erstellt?	☐	☐

Ist festgelegt worden, welche Webseiten gesperrt bzw. geblockt werden?	☐	☐
Ist bekannt, welche Einstellungen auf interne Internetkomponenten durch externe Dienstleister durchgeführt worden sind?	☐	☐
Werden die Internetkomponenten auch nach Dienstende überwacht?	☐	☐
Gibt es Regelungen (Ausdruck, Vorlage, Attachments) für die Behandlung von E-Mails?	☐	☐
Gibt es Regeln zur Verschlüsselung von E-Mails (in welchen Fällen, Organisation der Schlüsselverwaltung)?	☐	☐
Bestehen Notfallhandlungsanweisungen für die IT-Verantwortlichen?	☐	☐



Anhang

- Literaturverzeichnis
- Übersicht – Windows 2000 Resource Kit
- Bestellformular *backUP*-Magazine

Literaturverzeichnis

- Windows 2000 Server Insider, Umfassende Referenz für Netzwerkspezialisten
  Markt und Technik, William Boswell
- Windows 2000 Server, Installation, Konfiguration und Administration
  Microsoft Press, Original Microsoft Training
- Windows 2000 Design der Netzwerksicherheit
  Microsoft Press, Original Microsoft Training
- Windows-Sicherheit, Sicherheit von Systemen, Daten und Netzwerken
  Addison-Wesley, Kerstin Eisenkolb, Mehmet Gökhan, Helge Weickardt
- Windows 2000 Server, Das Handbuch
  Microsoft Press, Martin Kuppinger
- Windows 2000 Server, Kompendium
  Markt und Technik, Todd Brown, Chris Miller
- Windows 2000 Server, Einrichtung, Verwaltung, Referenz
  Win.tec, Eric Tierling
- Windows 2000 im professionellen Einsatz
  Hanser, Uwe Bünning, Jörg Krause
- Windows 2000 Server
  Data Becker, Christoph Lindemann, Christian Immler, Torsten Götz

Übersicht - Windows 2000 Resource Kit

Active Directory Replication Monitor: This utility graphically displays the replication topology of connections between servers on the same site.

Active Directory Schema Manager: The Schema Manager is a Microsoft Management Console (MMC) snap-in that allows you to view, modify, and extend the Active Directory schema.

Add Users: This 32-bit administrative tool for Windows 2000 uses a comma-delimited file to create, write, and delete user accounts.

Add Users to a Group: The UsrToGrp tool adds users to a local or global group according to information in a user-specified input text file.

ADSI Edit: ADSI Edit is a Microsoft Management Console (MMC) snap-in that acts as a low-level editor for the Active Directory.

Adsizer: Active Directory Sizer – Estimates the hardware required for deploying Active Directory in an organization.

Apimon: API Monitor – Monitors the API calls made by a process.

Appsec: Application Security Hotfix – Sets user permissions on a file-by-file basis to lock down accessible applications.

Associate: This command-line tool enables you to register or unregister a file name extension with the registry.

AuditPol: AuditPol is a command-line tool that enables the user to modify the audit policy of the local computer or of any remote computer.

AutoExNT Service: AutoExNT Service allows you to start a batch file, Autoexnt.bat, at boot time without having to log onto the computer on which it will run.

Batch File Wait: Sleep causes the computer to wait for a specified amount of time.

Browser Monitor: Browser Monitor is a GUI tool that monitors the status of browsers on selected domains. Browsers are shown on a per-domain and per-transport basis.

Browser Status: BrowStat is a general purpose, character-based browser diagnostic tool. Use BrowStat to find out whether a browser is running and to find active Microsoft Windows for Workgroups (WFW) browsers in Windows 2000 and Windows NT domains.

ChgPrint: Change Printer Utility – This tool assists network-administrators in managing printer shares. mains.

Clipstor: This GUI tool manages multiple Clipboard text buffers. It allows you to retrieve text from the Clipboard and store it in one of its buffers, and paste any of its buffers to the Clipboard, with your mouse.

Clusrest: Cluster Quorum Restore Utility – Restores the quorum disk of a cluster, which is not done by a restore process using NtBackup.

Cluster Verification Utility: Verifies that two-node cluster systems are set up properly.

CompReg: A Win32 character-based/command-line "Registry DIFF" that enables you to compare any two local or remote registry keys in Windows 2000, Windows NT, and Windows 95/98.

Ctrlist: Counter List – Lists all objects and counters installed in the system for the given language ID.

CustCon: Console Key Customizer – Custcon.exe is a Windows 2000 GUI tool that is used to customize the extended line editing keys when using Cmd.exe (Ntconsole). To enable new key settings, click the "Use Extended Edit Keys" checkbox.

Defptr: Default Printer – Using this tool you can easily change your default printer, switching between available network or local printers.

Delprof: User Profile Deletion Utility – This tool deletes user profiles on computers running Windows 2000.

Delrp: Delete File and Reparse Points – Deletes a file or directory and any associated NTFS reparse points.

Delsrv: Unregisters a service with the service control manager.

Dependency Walker: Dependency Walker is a graphical Win32 development tool that scans any Win32 module (.exe, .dll, .ocx, .cpl, .scr, and .sys, among others) and builds a hierarchical tree diagram of all dependent modules.

Dflayout: Compound File Layout User Tool – This layout tool for document files enables you to optimize compound files for improved performance over low-bandwidth networks, such as the Internet.

DH: Display Heap – Displays information about heap usage in a user-mode process or pool usage in kernel-mode memory.

DHCPCMD: DHCP Administrator's Tool – This command-line tool provides an auxiliary method of administering Dynamic Host Configuration Protocol (DHCP) servers.

Dhcpexim: DHCP Database Export Import Tool – Exports a DHCP database and server configuration from a server running Windows NT 4.0 Server or Windows 2000 Server for import into a destination DHCP server running Windows 2000.

DHCPLOC: DHCP Server Locator Utility – DHCP Server Locator Utility displays the DHCP servers active on the subnet. If it detects any unauthorized DHCP servers, it beeps and sends out alert messages.

DHCPOBJS: DHCP Objects – DHCP Objects allows you to automate DHCP Server configuration. It also provides enhanced capabilites over the Dhcpcmd tool, such as the ability to remove a DHCP lease.

Diruse: Directory Disk Usage – Displays information about a disk and the contents of its partition table.

Diskmap: Displays information about a disk and the contents of its partition table.

Diskpart: Diskpart Command Line Utility – Enables storage configuration from a script, remote session, or other command prompt.

DiskProbe: DiskProbe is a sector editor for Windows 2000. It allows a user with local Administrator rights to directly edit, save and copy data on the physical hard drive that is not accessible in any other way.

DiskUse: DiskUse is a command-line tool that scans directories on a hard disk and reports on space used by each user.

Dmdiag: Disk Manager Diagnostics – Saves disk volume configuration to a text file and writes a signature to a disk partition.

DNSCMD: DNS Server Troubleshooting Tool – Dnscmd.exe is a command line tool designed to assist administrators in DNS management.

DomMon: Domain Monitor – Domain Monitor monitors the status of servers in a domain and the secure channel status to the domain controller and to domain controllers in trusted domains.

Drivers: List Loaded Drivers – Displays information on installed device drivers, their files, and their code.

Drmapsrv: Drive Share Hotfix – Automatically configures NET SHARE and NET USE client drives for Terminal Services server access. **Note:** This download includes only the hotfix for the utility, not the tool itself.

DSACLS: This tool facilitates management of access-control lists for directory services.

DSASTAT: This diagnostic tool compares and detects differences between naming contexts on domain controllers.

Dumpel: Dump Event Log – Dumps an event log to a tab-separated text file.

Dumpfsmos.cmd: Dump FSMO Roles – Dumps the Flexible Single Master Operations roles.

Dureg: Registry Size Estimator – Shows how much data is stored in the registry, or in any registry subtree, key, or subkey.

DxDiag: DirectX Diagnostic Tool – This tool presents information about the components and drivers of the Microsoft DirectX application programming interface installed on your system.

Efsinfo: Encrypting File System Information – Displays information about encrypted files on NTFS partitions.

Exctrlst: Extensible Performance Counter List – Displays information on extensible performance counter DLLs installed on a computer.

ExeType: Finding the Executable Type – ExeType is a command-line application that identifies the operating system environment and processor required to run a particular executable file.

Expand: File Expansion Utility – This command-line tool enables you to expand files that have been compressed by Compress.exe.

Extract.exe: Extract Cabinet – Extracts files from cabinet (.cab) files.

FAZAM 2000: Reduced-Functionality Version – Extends Group Policy management functionality of Windows 2000.

File Compress: This command-line tool can compress one or more files.

FileVer: This command-line tool examines the version resource structure of a file or a directory of files on either a local or remote computer and displays information on the versions of executable files such as .exe files and dynamic-link libraries DLLs.

FindGrp: Find Group – This tool finds all direct and indirect group memberships for a specified user in a domain.

FlopLock: Lock Floppy Disk Drives – FloppyLock is a service that controls access to the floppy drives of a computer.

ForFiles: This command-line tool can be used in a batch file to select files in a folder or tree for batch processing.

FreeDisk: This command-line tool checks a disk drive for free space, returning a 0 if the specified amount of free space is available and a 1 if it is not.

FtEdit: FT Registry Information Editor – FTEdit is a GUI tool that allows you to create, edit, and delete fault tolerance sets for disk drives and partitions of local and remote computers.

GetFlags: Global Flags Editor – GFlags is a GUI tool that enables a developer or system administrator to edit the NtGlobalFlag settings for Windows 2000.

Getmac: GetMAC – Gets a computer's MAC (Ethernet) layer address and binding order.

Getsid: Get Security ID – Compares the security IDs of two user accounts.

GetType: GetType.exe is a command-line tool that allows you to detect what type of Windows software (workstation, server or domain controller) is installed on a computer.

Global: This command-line tool displays members of global groups on remote servers or domains.

Gpotool: Group Policy Verification Tool – Allows administrators to check Group Policy object integrity and monitor policy replication.

Gpresult: Group Policy Results – Displays information about the result Group Policy has had on the current computer and logged-on user.

GrpCpy: Group Copy – This GUI tool enables users to copy the usernames in an existing group to another group in the same or another domain or on a computer running Windows 2000.

Guid2obj: GUID to Object – Maps a GUID to a distinguished name.

Heapmon: Enables user to view system heap information.

Hlscan: Hard link display tool – Displays hard links on an NTFS volume or in specified files or directories of the volume.

Ifmember: Checks whether the current user is a member of a specified group.

IIS Migration Wizard: Migrates Web server configuration settings.

Installation Monitor: Tracks changes made by setup programs in the registry, .INI files, and other child processes.

IntBind: Interrupt Affinity Tool – The Interrupt Affinity Tool is used on multiprocessor systems to affinitize interrupts of disk or network adapters to one or more processors.

Inuse: File-In-Use Replace Utility – Performs on-the-fly replacement of files currently in use by the operating system.

Ipsecpol: Internet Protocol Security Policies Tool – Configures Internet Protocol Security (IPSec) policies in the Directory Service, or in a local or remote registry.

Kerbtray: Kerberos Tray – Displays ticket information for a given computer running the Kerberos protocol.

KernProf: Kernel Profiler – This command-line tool provides counters for and profiles of various functions of the Windows 2000 kernel.

Kill: Task Killing Utility – Use this command-line tool to end one or more tasks or processes. Use TLIST to find out the PID.

Klist: Kerberos List – Views and deletes the Kerberos tickets granted to the current logon session.

KSetup: Kerberos Setup – KSetup is a command-line tool for configuring Windows 2000 Professional to use an MIT-based Kerberos realm instead of a Windows 2000 domain.

KTPass: Kerberos Keytab Setup – KtPass is a configuration tool for MIT Kerberos interoperability that allows an Administrator to configure a non-Windows 2000 Kerberos service as a security principal in the Windows 2000 Active Directory.

LDP: Active Directory Administration Tool – Ldp is a graphical tool that allows users to perform Lightweight Directory Access Protocol (LDAP) operations, such as connect, bind, search, modify, add, and delete, against any LDAP-compatible directory, such as the Active Directory.

Leakyapp: This GUI testing tool appropriates system memory to see how other applications or the system as a whole runs in low-memory situations.

Link Check Wizard: Link Check Wizard scans all of the link (shortcut) files on your system, and checks to see if the shortcut points to an existing application or document.

LINKD: This command-line tool links an NTFS directory to a target object.

LIST: Text Display and Search Tool – This simple text display and search tool lists the contents of a file. Unlike other text display Tools, List is a good tool for looking at large text or log files because it does not read the whole file into memory when you open it.

LOCAL: This command-line tool displays members of local groups on remote servers or domains.

LogEvent: Event Logging Utility – This tool enables you to make entries to the Event Log on either a local or remote computer from the command prompt or a batch file.

LogOff: The LogOff tool is used to log a user off from the command prompt.

LogTime: This command-line tool logs the start or finish of command-line programs from a batch file. This can be useful for timing and tracking batch jobs such as mail-address imports.

MemSnap: Memory Profiling Tool – This memory profiling tool takes a snapshot of the memory resources being consumed by all running processes and writes this information to a log file.

MoveTree: Active Directory Object Manager – Movetree.exe is a command line tool that allows administrators to move Active Directory objects such as organizational units, users or computers between domains in a single forest.

MUNGE: This command-line tool provides a convenient way to search for and replace strings in a file or files.

NETAFX: Network Configuration Tool – This tool can be used to configure a variety of network parameters from the command prompt.

NetCmd: NetCmd.exe is a command-line tool that opens a command prompt. It automatically maps a UNC path to a drive letter. You can point to any folder in Windows Explorer (or any common file dialog) and open up a command prompt at that location.

NetCons: Net Connections – This GUI tool monitors and displays current net connections, taking the place of the Windows command-line command net use.

Netdiag: Network Connectivity Tester – Helps isolate networking and connectivity problems.

NetDom: Windows 2000 Domain Manager – This tool enables administrators to manage Windows 2000 domains and trust relationships from the command line.

Netsvc: Command-line Service Controller – You can use NetSvc to remotely start, stop, and query the status of services from the command line.

NetWatch: Net Watch shows which users are connected to shared folders. It also enables you to disconnect users and un-share folders. It can now simultaneously monitor multiple computers.

NLMon: This command-line tool can be used to list and test many aspects of trust relationships.

NLTest: This command-line tool helps perform network administrative tasks.

Now: Echoes the current date and time plus any arguments passed to it.

NSS2DOC: This utility helps the Remote Storage product in Windows 2000 Server migrate documents stored in the native structured storage (NSS) format to tertiary storage (tape).

Ntdetect.com: (Installd.cmd) – Installs a debug version of Startup Hardware Detector used for troubleshooting hardware detection issues.

NTDSUTIL: Directory Services Management Tool – NtdsUtil performs database maintenance of the Active Directory store, management and control of the Floating Single Master Operations (FSMO), and cleaning up of metadata left behind by abandoned domain controllers, those which are removed from the network without being uninstalled.

NTRights: With this command-line tool, you can grant or revoke any Windows 2000 right to or from a user or group of users.

NTUUCODE: 32-Bit UUDecode and UUEncode Utility – You can use this 32-bit GUI program to encode or decode files according to the UUEncoding standard.

Oh: Open Handles – Shows the handles of open windows, processes, or objects.

Oleview: OLE/COM Object Viewer – Browses, configures, and tests Microsoft Component Object Model classes installed on a computer.

PassProp: This command-line tool can be used to set two domain policy flags: whether passwords have to be complex and whether the administrator account can be locked out.

Pathman: Path Manager – Adds or removes components of the system or user path.

PerfMetr: Performance Meter – This command-line tool displays text-based information on the performance of a computer running Windows 2000.

PermCopy: This command-line tool copies share-level permissions (ACLs) from one share to another.

Perms: File Access Permissions per User – Displays a user's access permissions for a file or directory.

Pfmon: Page Fault Monitor – Lists the source and number of page faults generated by an application's function calls.

PMON: Process Resource Monitor – PMon is a command-line tool that monitors process resource usage, tracking CPU and memory usage.

PPTP Ping: Point-to-Point Tunneling Protocol Ping Tools – Pptpclnt.exe and Pptpsrv.exe are Tools that work in unison to verify that the required protocol and port for Point-to-Point Tunneling Protocol (PPTP) is being routed from a PPTP client to a PPTP server or vice-versa.

PrintMig: Printer Migrator – This printer configuration tool allows you to back up or migrate any print server on which you have administrative rights.

Pstat: Process and Thread Status – Shows the status of all running processes and threads.

PTree: Process Tree – Process Tree allows you to query the process inheritance tree and kill processes on local or remote computers.

Pulist: Lists processes running on local or remote computers.

PViewer: Process Viewer – Process Viewer is a Windows-based tool that displays information about a running process and allows you to stop (kill) processes and change process priority.

Qslice: CPU Usage by Processes – Shows the percentage of total CPU usage per process.

RASList: This command-line tool displays Remote Access Service (RAS) server announces from a network.

RASMon: You can use this tool to monitor your Remote Access Service.

RASUsers: Enumerating Remote Access Users – RasUsers lets you list for a domain or a server all user accounts that have been granted permission to dial in to the network via Remote Access Service (RAS).

Rdpclip: File Copy Hotfix – Copies files between Terminal Services server and client.

REG: This tool enables you to add, change, delete, search, backup, restore, and perform other operations on registry entries from the command prompt or a batch file. It can be used on both local and remote computers.

REGBack: Registry Backup – Registry Backup (RegBack) is a tool for backing up the Windows Registry to files without use of a tape drive. RegBack allows you to back up Registry hives while the system is running and has the hive files open.

REGFind: RegFind is a command-line tool with which you can search the Windows 2000 registry for arbitrary data, key names, or value names and optionally replace any of these with new values.

REGINI: Registry Change by Script – This tool uses character-based batch files to add keys to the Windows 2000 registry by specifying a registry script.

REGRest: Registry Restoration – Registry Restoration (RegRest) restores Registry hive files from backups created by RegBack.

Relog: Extracts performance counters from logs created by the Performance Logs and Alerts service.

ReMapKey: Remap Windows Keyboard Layout – This tool changes keyboard layout by re-mapping the scancode of keys.

Remote Command Service: Rcmd.exe & Rcmdsvc.exe – The Remote Command Service (Rcmd.exe) provides a secure, robust way to remotely administer and run command-line programs. (RCMDSRV also included.)

Remote Administration Scripts: The Remote Administration Scripts are a collection of Visual Basic scripting Tools designed to perform specific administrative tasks using Microsoft Active Directory Services Interfaces (ADSI) and Windows Management Instrumentation (WMI) for Windows 2000. Rscripts.chm is an HTML Help file that documents the Remote Administration Scripts.

RKill: Remote Kill – This service (RKILLSRV.EXE) with both GUI (WRKILL.EXE) and command-line (RKILL.EXE) clients allows a user to enumerate and kill processes on a remote computer. To kill a process remotely with this tool, you must be member of the Administrators group.

RMTShare: Remote Share – Remote Share is a command-line tool that allows you to set up or delete shares remotely.

RPCCfg: RPC Configuration Tool – Configures Microsoft Remote Procedure Call (RPC) to listen on specified ports.

Rpcdump: RPC Dump – Dumps all endpoints in the endpointmapper database, pings each endpoint, gathers other stats, sorts and displays the data.

RPC Ping: RPC Connectivity Verification Tool – Verifies that Windows 2000 Server services are responding to remote procedure call requests from network clients.

RSDiag: Remote Storage Diagnostic Utility – This command-line tool examines Remote Storage (HSM) databases and displays diagnostic information about jobs, managed NTFS 5 volumes, removable media, and other Remote Storage information useful for system analysis.

RSDir: Remote Storage File Information Utility – This command-line tool examines Remote Storage reparse points, displaying Remote Storage information for files in the current directory and its subdirectories.

SC: Service Controller Query Tool – This tool provides a way to communicate with Service Controller (Services.exe) from the command prompt to retrieve information about services.

ScanReg: This Win32 command-line "registry GREP" enables you to search for any string in keynames, valuenames, and/or valuedata in local or remote registry keys in Windows 2000 Windows NT, and Windows 95/98.

ScList: This command-line tool can show currently running services, stopped services, or all services on a local or remote computer.

SecAdd: This command-line tool enables you to add user permissions to a registry key or removed "Everyone" group.

Setspn: Manage Service Principal Names for an Active Directory directory service account.

SetupMgr: Setup Manager – This wizard is a deployment tool that assists system administrators in automating the installation or upgrading of Windows 2000 on multiple computers, eliminating the need to monitor these operations.

Setx: Sets environmental variables in the the user or computer environment.

ShowACLs: This command-line tool enumerates access rights for files, folders, and trees. It allows masking to enumerate only specific ACLs.

ShowDisk: This command-line tool reads and displays the registry subkey HKEY_LOCAL_MACHINE\SYSTEM\DISK.

ShowGroups: This command-line tool shows the groups to which a given user belongs, optionally within a given network domain.

ShowMembers: This command-line tool shows the usernames of members of a given group, optionally within a given network domain.

Showperf: Performance Data Block Dump Utility – Dumps the contents of the Performance Data block so you can view and debug the raw data structure.

ShutDown: Remote Shutdown – Remote Shutdown is a command-line tool that allows you to remotely shut down or reboot a computer running Windows 2000.

ShutGUI: Remote Shutdown GUI – Shutgui.exe allows you to remotely shut down or reboot a computer running Windows 2000. It can be run either with command-line parameters or without.

SIDwalker: This set of programs helps system administrators manage access-control policies on Windows 2000 and Windows NT systems. Access control is implemented by access-control lists (ACLs).

SNMP Monitor: SNMP Monitor is a tool that can monitor any SNMP MIB variables across any number of SNMP nodes.

SNMPutil & SNMPutilG: SNMP Browser is a tool that lets you get SNMP information from an SNMP host on your network. SnmpUtilG is a graphical tool that complements the older command prompt SNMP browser tool (Snmputil.exe).

Soon: Near-Future Command Scheduler – Schedules commands to run within the next 24 hours.

Applications as Services Utility: With **Srvany**, you can configure any Windows application so that it runs as a service.

SrvCheck: This command-line tool lists the non-hidden shares on an computer running Windows 2000 and enumerates the users on the ACLs for that share.

SrvInfo: This command-line tool displays information, such as available disk space and partition types, about a remote server.

SU: SU lets you start a process running as an arbitrary user. It is named after the SU (Switch Users) utility of the UNIX family of operating systems.

SubInAcl: With this command-line tool, administrators can obtain security information on files, registry keys, and services, and transfer this information from user to user, from local or global group to group, and from domain to domain.

SvcMon: Service Monitoring Tool – This tool monitors services on local and remote computers for changes in state (starting or stopping).

Sysdiff: Automated Installation Tool Hotfix – Pre-installs applications as part of an automated setup.

SysPrep: Use this tool to prepare your system before changing SID using SIDwalker.

TakeOwn: TakeOwn is a command-line tool that cleans up multiple boot drives without formatting the drive. Using this tool, you can delete an installation of Window 2000 from a local computer.

TextViewer: TextViewer provides a graphical interface for quickly viewing text files on local or shared drives.

Timethis: Times how long it takes to execute a given command.

Tracedmp: Processes a trace log file or real time trace buffers and converts them to a .csv file.

Traceenable: Enables tracing and displays current tracing options.

Tracelog: Starts, stops or enables trace logging.

Terminal Server Capacity Planning Tools: Hotfix – Suite of Tools that assist organizations with Windows 2000 Terminal Services capacity planning.

TimeOut: Timeout is a command-line tool that causes the command processor to pause execution for the number of seconds specified by the time (#) parameter, after which it continues without requiring a user keystroke.

TimeThis: TimeThis times how long it takes the system to execute a given command.

Timezone: Daylight Savings Time Update Utility – This command-line tool updates the daylight savings information for a time zone in the registry.

TrustDom: Trust Domain Setup – This command-line tool can help manage trust relationships. Using TrustDom, administrators can view, create, and delete trust relationships between Windows 2000 and Windows NT domains.

TypePerf: Performance Data in the Command Window – This command-line tool displays real-time data from Performance Monitor counters in a command window.

TZedit: Time Zone Editor – You can use Time Zone Editor to create and edit time zone entries for the Date/Time option in Control Panel.

UserDump: User Mode Process Dumper – UserDump.exe is a command-line tool that creates a dump file for user mode debugging. UserDump does not use Dr. Watson and does not invade the target process as a debugger.

User Input for Batch Files: Choice prompts the user to make a choice in a batch program by displaying a prompt and pausing for the user to choose from among a set of keys.

User State Migration Tool: Helps migrate a user's documents and settings (state) before an operating system migration to Windows 2000.

UsrStat: This command-line tool displays the username, full name, and last logon date and time for each user in a given domain.

Vadump: Virtual Address Dump – Shows the state and size of each segment of virtual address space.

Vfi: Visual File Information – Visual File Information retrieves and generates file information.

W3who.dll: Browser Client Context Tool – ISAPI application DLL that displays the browser client context. Lists security identifiers, privileges, env variables.

WaitFor: This command-line tool waits until a signal is given across the network. Multiple machines can wait for the same signal.

Whoami: Returns the domain or computer name and the user name of the user currently logged onto the computer on which the tool runs.

WinAt: Command Scheduler – Command Scheduler can be used to schedule commands on a local or remote computer to occur once or regularly in the future.

WinDiff: File and Directory Comparison – WinDiff shows the differences between specified ASCII text files or folders of ASCII text files.

Winexit: Windows Exit Screen Saver – WinExit is a screen saver that logs the current user off after the specified time has elapsed.

Windows ATM ARP Server Information Tool: AtmArp is a command-line tool designed to assist network administrators and support personnel in troubleshooting the status of the Asynchronous Transfer Mode (ATM) ARP/MARS Service that ships with Windows 2000.

Windows ATM LAN Emulation Client Information: AtmLanE is a command-line tool designed to assist administrators in troubleshooting the status of the Asynchronous Transfer Mode (ATM) LAN Emulation (LANE) client that ships with Windows 2000.

WinMsDp: WinMsdp is a command-line version of the Windows 2000 Diagnostics tool (Winmsd.exe). It provides information about your system configuration and status.

WINS Administrator Tools: WinsCl can monitor WINS activities and examine WINS databases. It can also send commands to WINS to initiate an activity such as replication, scavenging, registering/querying a record, or doing backup/restore operations.

WinSCHK: This command-line tool checks name and version-number inconsistencies that may appear in Windows Internet Name Service (WINS) databases, monitors replication activity, and verifies the replication topology in an enterprise network. It is particularly useful for WINS administrators.

Winsta: WinStation Monitor – Monitors the status of all users logged on to a Windows 2000 Terminal Server.

Wntipcfg: Windows NT IPConfig Utility – Gives you information about your IP configuration.

Xcacls: Sets all file-system security options accessible in Windows Explorer.

Bestellformular ***backUP***-Magazine für IT-Sicherheit
***backUP*-Magazine erhalten Sie kostenlos!**
Fax: 0431/988-1223 **Mail:** mail@datenschutzzentrum.de **Internet:** http://www.datenschutzzentrum.de
Absender:
Magazine:
☐ **Nr. 1: IT-Sicherheitskonzepte** Planung – Erstellung – Umsetzung
☐ **Nr. 2: MS-Windows NT 4.0** Sicherheitsmaßnahmen und Restrisiken
☐ **Nr. 3: MS-Windows NT 4.0** Resource Kit und Security-Tools
☐ **Nr. 4: PC-Arbeitsplatz** So viel Datenschutz muss an jedem Arbeitsplatz sein!
☐ **Nr. 5: MS-Windows 2000** Sicherheitsmaßnahmen und Restrisiken
☐ **Bitte nehmen Sie mich in den Verteiler *backUP*-Magazine auf.**