



Benutzermanagement

Beron Robert

Veröffentlicht: April 2003

Installationsanleitung für den Einsatz der im Microsoft-BM:BWK Schoolagreement enthaltenen Serverprodukte

Abstract

[Abstract Text]

1. Zugriff auf Dateiressourcen

1.1. Berechtigungen auf Dateien oder Ordnern

Bei der Installation des Betriebssystems wurde das Dateisystem ausgewählt. Als Standard wird dabei das Windows 2003 Servereigene Dateisystem **NTFS**¹ vorgeschlagen. Durch diese Auswahl haben Sie ein stabiles, transaktionsorientiertes Dateisystem gewählt dass weitergehende Funktionen wie z.Bsp. Vergabe von Berechtigungen auf Dateien und Ordner oder Überwachung der Zugriffe enthält.

Berechtigungen dienen dem Schutz von Dateien, Ordnern oder Netzwerkressourcen. Mit ihnen erlaubt man Gruppen oder Benutzern den Zugriff auf Ressourcen, gleichgültig, ob der Zugriff über das Netzwerk oder lokal² erfolgt.

Aus einer Vielzahl von Einzelberechtigungen wurden **Standardberechtigungen** definiert, die der Administrator oder Besitzer eines Objektes vergeben kann.

- **Lesen:** Lesen einer Datei bzw. Anzeige der Dateiattribute, der Berechtigungen oder Anzeige des Besitzers.
- **Schreiben** Mit dieser Berechtigung kann die Datei überschrieben werden. Daneben werden auch Besitz und Berechtigungen angezeigt.
- **Lesen, Ausführen:** Diese Berechtigung ist notwendig, um Programme ausführen, also starten zu können.
- **Ändern:** Neben dem Lesen, Schreiben, Ausführen umfasst diese Berechtigung noch das Ändern und Löschen von Objekten wie z.B. einer Datei oder einem Ordner.
- **Vollzugriff:** Diese Berechtigung stellt die höchst mögliche aller Berechtigungen dar und **enthält alle anderen Berechtigungen** sowie die Möglichkeit der Übernahme des Besitzes an einem Objekt.

Bei Ordner-Berechtigungen kommt, im Gegensatz zu Datei-Berechtigungen, noch die Berechtigung **Ordnerinhalte auflisten** hinzu. Durch diese Berechtigung werden die Dateien in einem Ordner und die Unterordner des Ordners aufgelistet.

Üblicherweise werden Berechtigungen über domänen-lokale oder lokale Gruppen vergeben.

Der Grund liegt in darin, dass i.d.R weniger Gruppen als Benutzer in einem Netzwerk angelegt sind. Gruppen werden meist nach **logischen, funktionellen,**

¹ NTFS (New Technology File System)

² Lokal auf einem Server können sich nur Administratoren und Benutzer die der Gruppe der Operatoren angehören anmelden.

organisatorischen Gesichtspunkten gebildet. Benutzer, die einer bestimmten Gruppe angehören, haben damit auch identische Zugriffsberechtigungen.

Wenn Sie die Berechtigungen einsehen oder ändern wollen, müssen Sie zuerst das gewünschte Objekt im Dateisystem auswählen und durch einen Rechtsklick das Kontextmenü aufrufen. In dem sich öffnenden Menü wählen Sie die Funktion **EIGENSCHAFTEN** aus.

In dem sich öffnenden Fenster wechseln Sie in das Register **SICHERHEIT**, in dem Sie die Berechtigungen des Objektes einsehen bzw. ändern können.

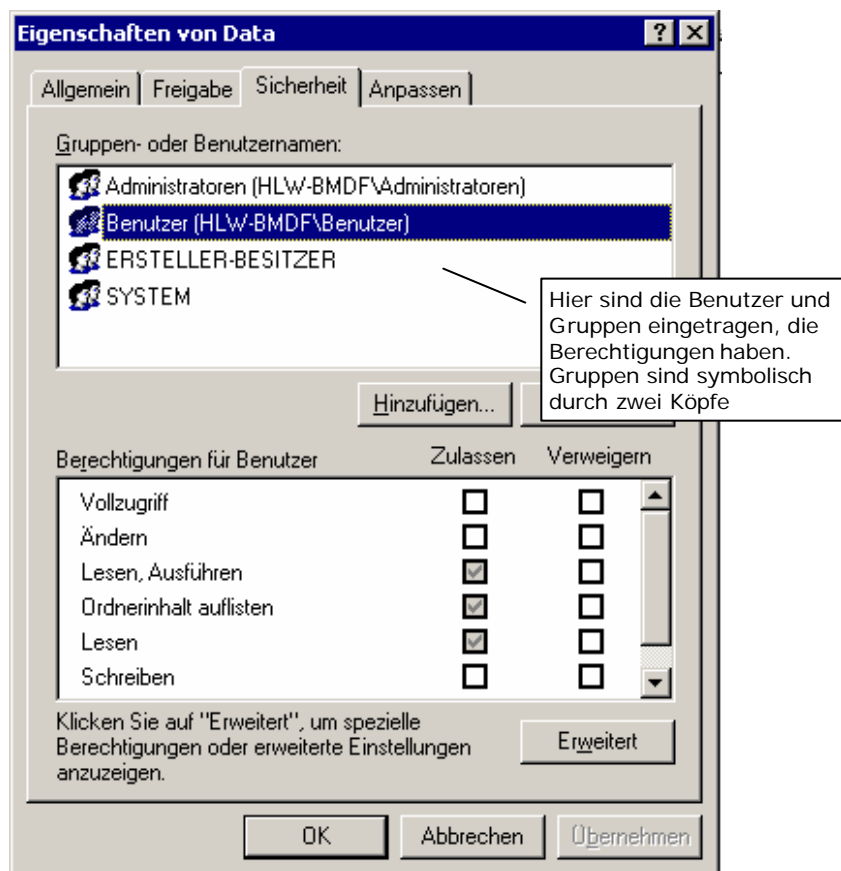


Abbildung: Anzeige der Sicherheitseinstellungen



Anmerkung: Windows 2003 Server arbeitet mit **vererbaren Berechtigungen**, d.h., dass ein Objekt die Berechtigungen des darüber liegenden Ordners erbt. Mit der Erstellung eines Ordners erbt dieser die Berechtigungen des übergeordneten Ordners.

Ob eine Berechtigung vererbt wurde oder nicht, können Sie leicht an der angehakten Kontrollboxen ersehen. Vererbte Berechtigungen sind angehakt und grau unterlegt.

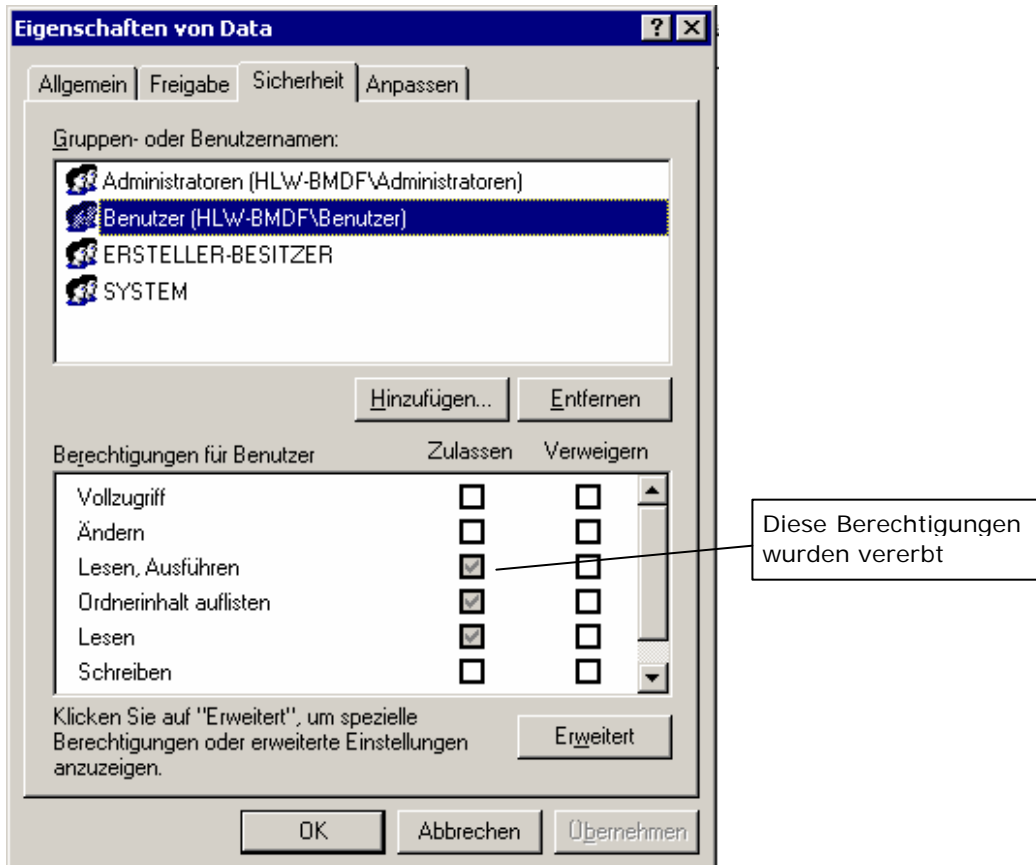


Abbildung: Eigenschaften eines Ordners – Berechtigungen der Gruppe „Benutzer“ sind vererbt und deaktiviert.

Um die Berechtigung der Gruppe „Benutzer“ zu ändern, muss zuerst die Vererbung ausgeschaltet werden. Mit einem Klick auf die Schaltfläche **ERWEITERT** gelangen Sie in die Erweiterten Sicherheitseinstellungen des Ordners „Data.“ Im unteren Abschnitt des Fensters müssen Sie die Kontrollbox „Berechtigungen übergeordneter Objekte, über ...“ enthaken. (siehe Abbildung).

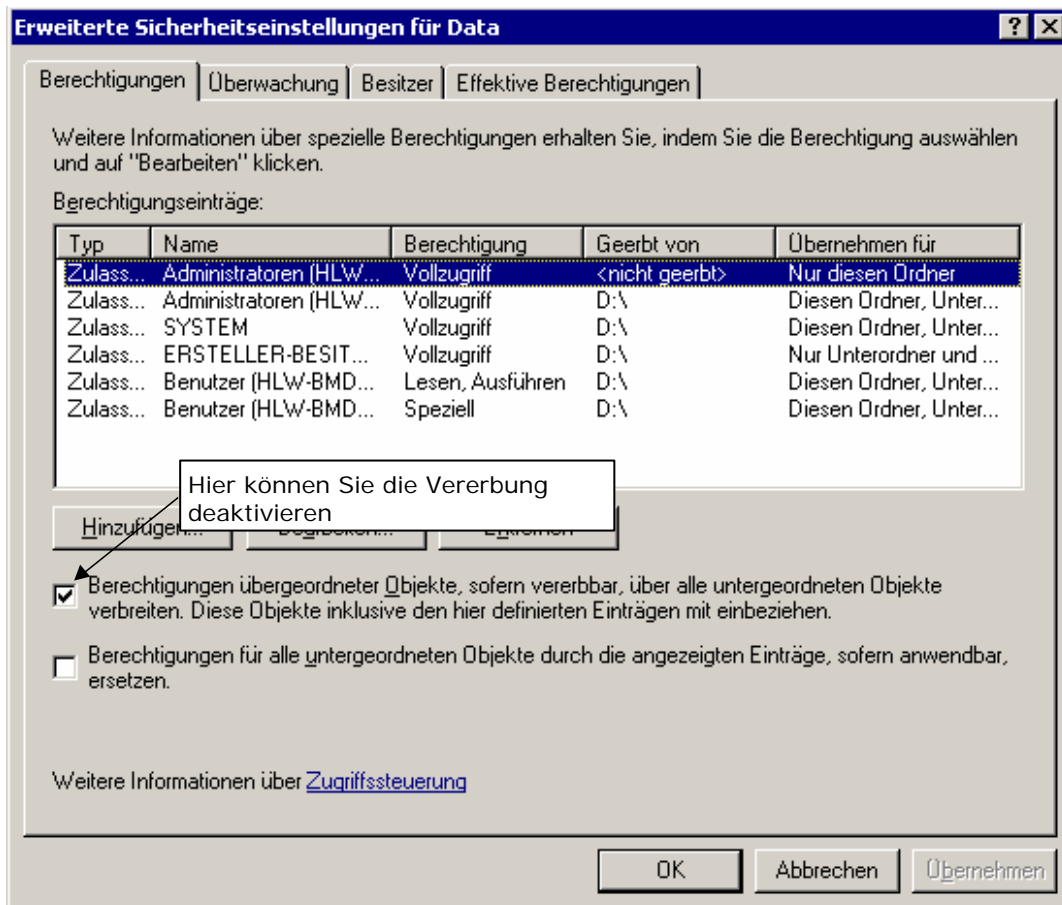


Abbildung: Erweiterte Sicherheitseinstellungen eines Ordners

Nach dem Klick auf die Kontrollbox erhalten Sie eine Meldung des Betriebssystems, dass ab nun die Vererbung nicht mehr angewandt wird. Je nachdem, ob Sie die vererbten Rechte übernehmen oder alle Sicherheitseinstellungen für diesen Ordner löschen wollen, müssen Sie entweder die Schaltfläche **KOPIEREN** oder **ENTFERNEN** anklicken.

Welche Berechtigungen im Einzelnen durch das Setzen der Kontrollbox einer Standardberechtigung wirklich vergeben werden, können Sie im oberen Teil des Fensters ersehen. Wenn Sie einen detaillierten Überblick wollen, so müssen Sie lediglich den Benutzer oder die Gruppe anklicken und anschließend die Schaltfläche **BEARBEITEN ...** wählen.

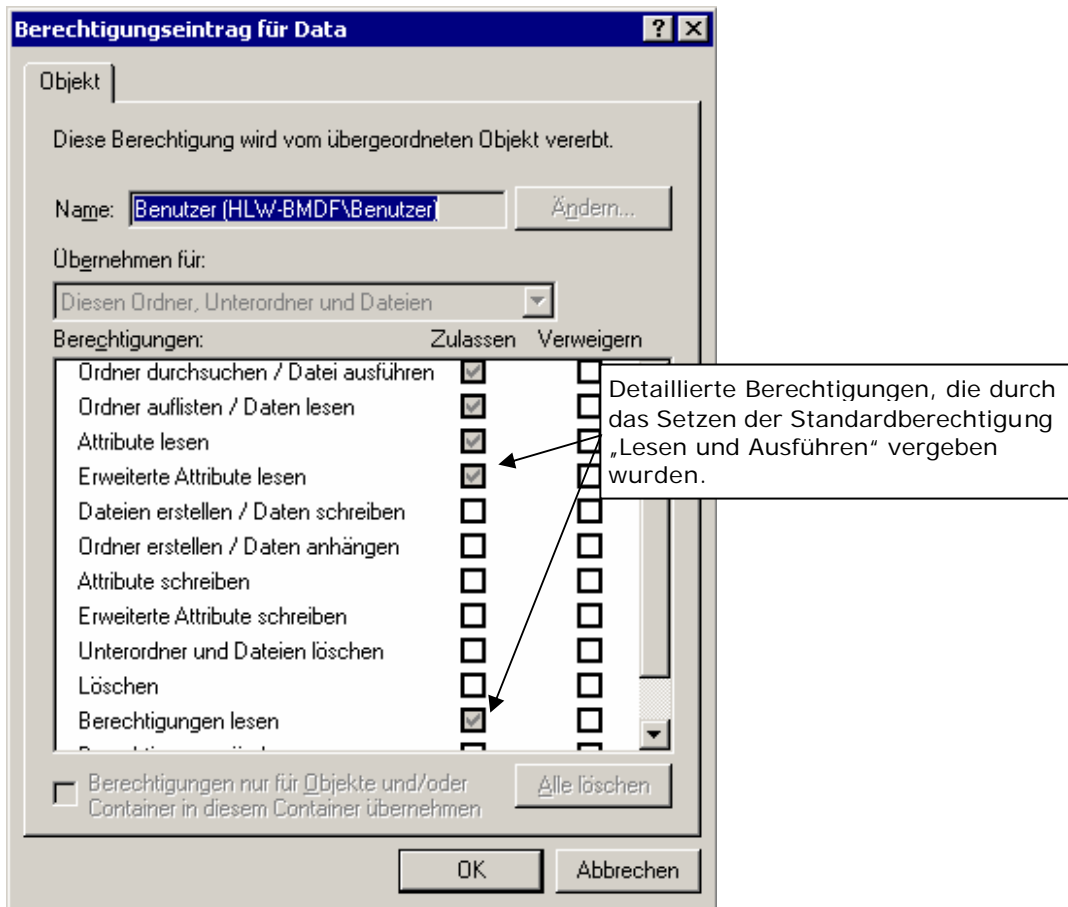


Abbildung: Berechtigungseintrag für eine bestimmte Gruppe

Die **effektive Berechtigung** eines Benutzers setzt sich aus den einzelnen Berechtigungen, die er durch die Mitgliedschaft in unterschiedlichen Gruppen erhalten hat, zusammen. Alle Berechtigungen addieren sich dabei, wobei das Verweigern der Berechtigung eine höhere Priorität hat als das Zulassen einer Berechtigung!

Unter Windows 2003 Server haben Sie nun endlich die Möglichkeit, die effektiven Berechtigungen eines Benutzer oder einer Gruppe sofort zu ermitteln.

Im Register **EFFEKTIVE BERECHTIGUNGEN** des Fenster „Erweiterte Sicherheitseinstellungen für ...“ können Sie sofort die effektiven Berechtigungen ermitteln. Nachdem Sie auf das Register geklickt haben, müssen Sie über die Schaltfläche **AUSWÄHLEN...** den Benutzer oder die Gruppe eingeben, für die Sie die effektiven Berechtigungen ermitteln wollen.

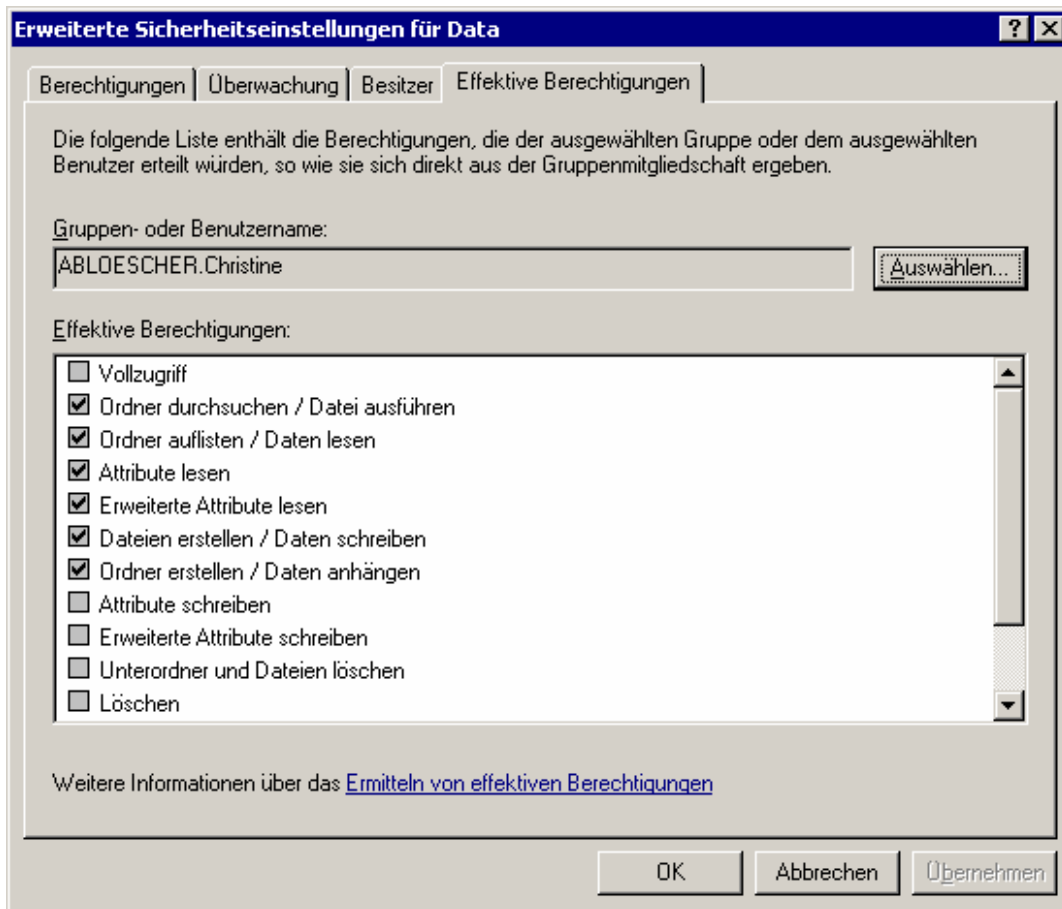


Abbildung: Effektive Berechtigungen des Benutzers Ablöschner Christine für einen bestimmten Ordner

Üblicherweise haben Dateien durch Vererbung die Berechtigung des übergeordneten Ordners. Dies kann allerdings auch geändert werden. Die Zugriffsberechtigung auf eine Datei kann ausgedehnt oder auch eingeschränkt werden!

1.2. Best Practice

- Vergeben Sie die Rechte ausschließlich über Gruppen. Vorzugsweise sollten Sie dazu lokale oder domänen-lokale Gruppen verwenden.
- Ersetzen Sie die Gruppe Jeder aus dem Root-Ordner der Festplatte durch die Gruppe der Server Operatoren.
- Vergeben Sie nur jene Rechte die eine bestimmte Benutzergruppe wirklich benötigt.
- Vergeben Sie niemals Rechte an einen Benutzer! Richten Sie in diesem Fall lieber eine zusätzliche Gruppe ein.

1.3. Freigabe von Ressourcen im Netzwerk

Sie arbeiten auf dem Server „\\srv01“ und wollen anderen Benutzern im Netzwerk den Zugriff auf den Ordner „D:\Data\InfoShare“ erlauben.

Zuerst öffnen Sie den Explorer und markieren das freizugebende Objekt im linken oder rechten Teil. Mit einem Rechtsklick wählen Sie aus dem Kontextmenü die Funktion **FREIGABE UND SICHERHEIT ...** aus.

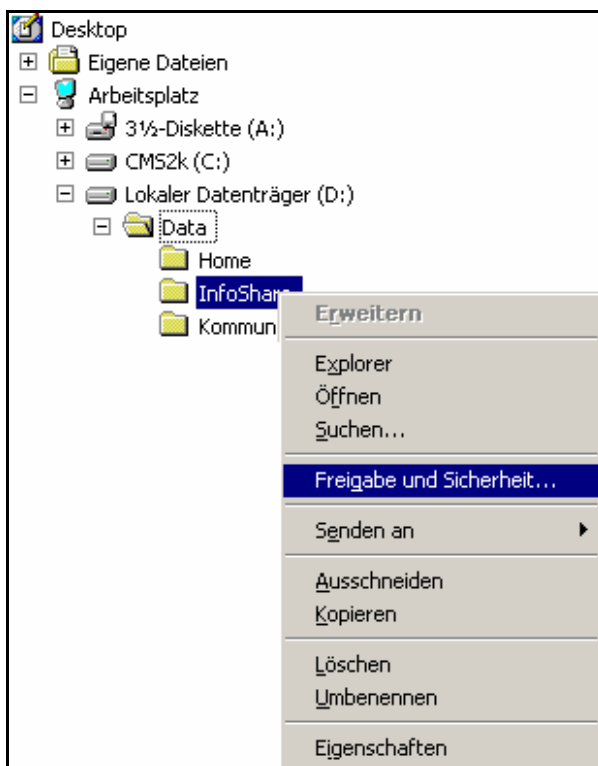


Abbildung: Explorer mit dem freizugebenden Ordner und seinem Kontextmenü (Ausschnitt)

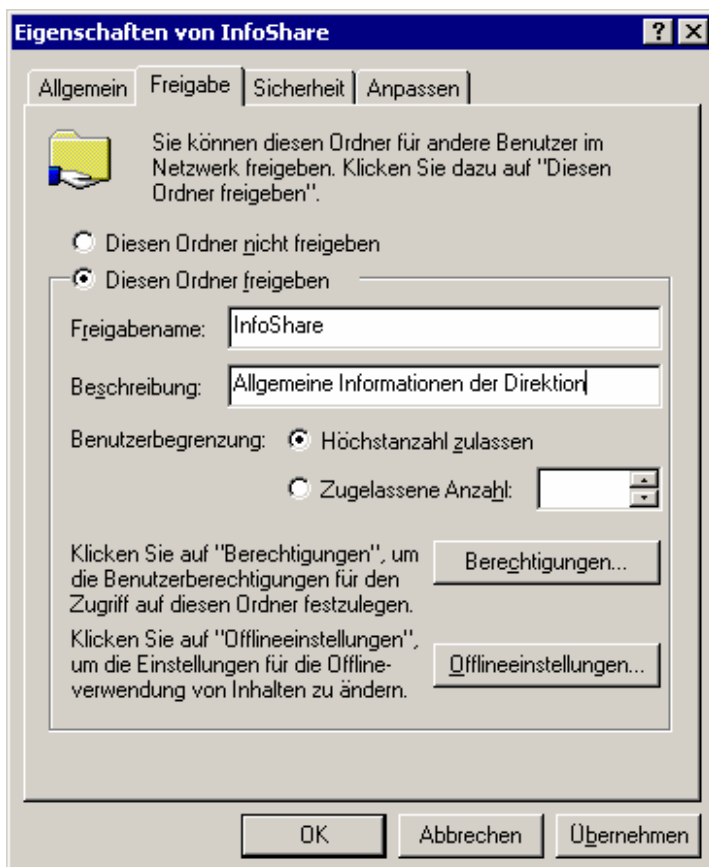
In dem sich öffnenden Fenster müssen Sie zuerst die Option „**Diesen Ordner freigeben**“ wählen, worauf im Textfeld „Freigabename“ der Name des Ordners vorgeschlagen wird.

Da sicherlich viele Ordner freigegeben werden, ist es sehr hilfreich, wenn Sie den freigegebenen Ordner mit einem Kommentar versehen. Dieser Kommentar ist für Benutzer gedacht und hilft diesen bei der richtigen Wahl des Ordners.

Neben dem Freigabennamen des Ordners und einem Kommentar können Sie auch **Berechtigungen** auf diesen Ordner vergeben und die **Anzahl der gleichzeitigen Zugriffe**³ einschränken.

Die Auswahl der möglichen Berechtigungen auf Freigabeebene mit **Lesen**, **Ändern** und **Vollzugriff** sind identisch mit denen auf NTFS – Dateisystemebene. Allgemein wird als Freigabeberechtigung **Jeder** mit **Vollzugriff** automatisch eingetragen. Um sich die Ermittlung des **effektiven Rechts** zu ersparen, wird i.d.R. die vorgeschlagene Freigabeberechtigung – Jeder, Vollzugriff - übernommen.

Das effektive Recht eines Benutzers setzt sich aus den NTFS-Dateisystemberechtigungen und den Freigabeberechtigungen zusammen. Der Benutzer erhält dabei aus beiden Berechtigungen die jeweils geringere Berechtigung.



³ Während die Anzahl der gleichzeitigen Zugriffe auf Windows 2003 Server unbegrenzt ist, ist die maximale Anzahl auf einen unter Windows XP Professional freigegebenen Ordner mit **10 Benutzern** begrenzt.

Abbildung: Freigabe eines Ordners mit dem Freigabennamen Infoshare und einem entsprechenden Kommentar

Freigegebene Objekte, in diesem Fall der Ordner „Infoshare“, werden durch eine „reichende“ Hand unter dem Symbol dargestellt. Neben Ordnern könnten Sie auch andere Objekte wie z.B. eine Festplatte, ein CD-ROM Laufwerk oder einen lokalen Drucker für andere freigeben. Der Vorgang ist dabei in allen Fällen der gleiche.



Anmerkung: Fügen Sie dem Freigabennamen ein \$-Zeichen hinzu, wird die Ressource versteckt. Nur Anwender, die den genauen Namen der Ressource kennen, können dann darauf zugreifen.

1.4. Best Practice

Welche File Ressourcen in einem Netzwerk freigegeben werden müssen ist von Schule zu Schule unterschiedlich und kann allgemein nicht beantwortet werden.

Eine allgemeine Empfehlung könnte dabei sein:

- Homeverzeichnis, also die persönlichen Ordner, der Benutzer sollten versteckt freigegeben werden. Auf diese haben nur die Gruppe Administratoren und der jeweilige Benutzer Vollzugriff.
- Ein allgemeines Kommunikationsverzeichnis für Schüler. Je nach Ausbildungsstand von Schülern oder Lehrer sollte entweder nur Ändern oder eventuell Vollzugriff gewährt werden. Achtung: Wenn Sie Vollzugriff gewähren können Benutzer die Ordner anlegen selbst Rechte auf diesen Ordner vergeben.
- Evt. pro Klasse ein eigener Kommunikationsordner. Ein alternative dazu wären Unterordner mit entsprechenden Rechten im allgemeinen Kommunikationsverzeichnis.
- Ein allgemeines Kommunikationsverzeichnis für Lehrer (Schüler haben hier keinen Zugriff)
- Ein Ordner für die Ablage der Schularbeiten. Schularbeitsdateien können hier abgelegt und gesichert werden. Auf diesen Ordner sollten nur Lehrer mit dem Recht Ändern zugriff haben.
- Ein freigegebener Verwaltungorder für Angestellte der Verwaltung. Bei Bedarf können weitere Unterordner für unterschiedliche Tätigkeitsbereiche Direktion, Schuladministration, Klassenvorstände usw. erstellt werden.
- Order für die Installation von Programmen.
- Etc ...





































 Biblio	Für Bibliothekarinnen
 BKVWIN	Wirtschaftsleitung
 Bonappetit	ÜFA Bonappetit
 DrDion	Nur für die Direktion
 Drucker0	Für den praktischen Bereich & Übungsfirmen. Kein allgemeiner Drucker!
 Drucker1	Für alle
 Drucker2	Für alle
 Drucker3	Für alle
 Drucker4	Für alle
 Drucker5	Für alle
 Drucker6	Für alle
 Drucker7	Für alle
 Drucker8	Für alle
 Drucker9	Nur für die Schüler der Notebook Klasse + Angestellte
 Drucker5	Für alle
 DruckerW	Erdgeschoß (Wirtschaftsleitung)
 FarBLaser	Nicht für den allgemeinen Gebrauch
 Lehrer	Drucker steht ausschliesslich dem Kollegium und den Angestellten zur Verfügung
 Lehrer_Kommunikation	Kommunikationsverzeichnis für Lehrer
 Mediendesign	ÜFA Mediendesign
 NETLOGON	Logon server share
 OKOMAT	Übernahmeverzeichnis für SKV
 PC_NT_DB	Common share for administrative tasks
 Personalentwicklung	ÜFA Personalentwicklung
 Reisebüro	ÜFA Reisebüro
 Schularbeiten	Sicherungsordner für Schularbeiten
 Schüler_Kommunikation	Allgemeins Kommunikationsverzeichnis für Schüler
 Schülerprogramme	Programme für Schüler
 SKVWin	Schülerküchenprogramm SKV
 SYSVOL	Logon server share
 TClient	Terminal Server Client
 Tourismus	Projektordner für Kulturtouristik
 Verwaltung	Verwaltungsbereich der Schule
 Video	Ordner für Video Projekte
 Printers	Adds, removes, and configures local and network printers
 Scheduled Tasks	Schedules computer tasks to run automatically

Abbildung: Beispielhafte Freigaben eines File Servers