Inhaltsverzeichnis

1. Zugriffsteuerung 2
2. Ordner- und Dateiberechtigungen 3
   2.1. NTFS – Ordnerberechtigungen: (siehe Abbildung 2-1) 3
   2.2. NTFS – Dateiberechtigungen: (siehe Abbildung 2-2) 4
   2.3. Erweiterte Berechtigungen: (siehe Abbildung 2-3 und Abbildung 2-4) 5
3. Hierarchie der Berechtigungen 7
   3.1. Explizite Berechtigungen – werden direkt an ein Objekt oder eine Organisationseinheit gebunden: (siehe Abbildung 3-1). 7
   3.2. Vererbte Berechtigungen – werden von einem übergeordneten auf ein untergeordnetes Objekt weitervererbt: (siehe Abbildung 3-2). 7
   3.3. Effektive Berechtigungen – die effektiven Berechtigungen eines Benutzers für eine bestimmte Ressource setzen sich aus der Summe der NTFS-Berechtigungen zusammen, die Sie einem einzelnen Benutzerkonto auf allen Gruppen gewähren, denen der Benutzer angehört: (siehe Abbildung 3-3 und Abbildung 3-4) 8
   3.4. Deaktivieren der Berechtigungsvererbung: 9
   3.5. Außerkraftsetzung von Ordnerberechtigung durch Dateiberechtigungen: 11
   3.6. Außerkraftsetzung von Berechtigungen durch eine Berechtigungsverweigerung: 12
4. Kopieren von Dateien und Ordnern 13
   4.1. Kopieren einer Datei innerhalb eines NTFS-Volumes oder zwischen zwei NTFS-Volumes: (siehe Abbildung 4-1) 13
5. Verschieben von Dateien und Ordnern 14
   5.1. Verschieben innerhalb eines NTFS-Volumes: (siehe Abbildung 5-1) 14
   5.2. Verschieben zwischen zwei NTFS-Volumes: (siehe Abbildung 5-2) 15
6. Besitzer für Dateien und Ordner 16
7. Verwalten freigegebener Ordner 17
   7.1. Voraussetzungen 17
   7.2. Freigeben eines Ordners 19
   7.3. Verbindungsherstellung zu einem freigegebenen Ordner 20
      Allgemeine Informationen zum Verbinden eines Netzlaufwerkes 20
      „Für Faule“: Mounten durch „browsen“ in der Netzwerkumgebung 20
      „Standardverfahren“: Mounten über den Explorer (Extras → Netzlaufwerk verbinden) 21
      „Für Profis“: Mounten über Kommandozeile und dem „net use“ Befehl 21
      „… nur mal schnell“: Mounten über UNC ohne Laufwerksbuchstaben 22
      „Für Esoteriker“: Mounten „unterhalb“ der Netzwerkumgebung 22
   7.4. Administrative Ordnerfreigaben 23
   7.5. Übersicht der Freigaben 23
   7.6. Trennen der Netzwerklaufwerke 24
   7.7. Anwenden von Berechtigungen für freigegebene Ordner 24
8. Überwachung 25
   8.1. Zusammenfassung: Richtlinien für die Berechtigungsvergabe bei freigegebenen Ordnern 26
   8.2. Offlinezugriff auf Dateien im Netz 27

1. Zugriffsteuerung

Wenn Sie einen Computer und seine Ressourcen schützen möchten, müssen Sie berücksichtigen, über welche **Rechte** die Benutzer verfügen sollen. Sie können einen oder mehrere Computer schützen, indem Sie Benutzern oder Gruppen bestimmte Benutzerrechte erteilen. Sie können ein Objekt, beispielsweise eine Datei oder einen Ordner, schützen, indem Sie **Berechtigungen** zuweisen, die es Benutzern oder Gruppen ermöglichen, bestimmte Aktionen für das Objekt auszuführen.

Rechte – Windows-Benutzerrechte bestimmen, welche Privilegien der Benutzer hat, um mit dem Betriebssystem zu interagieren (z. B. Herunterfahren des Systems, Installieren von Software, lokale Anmeldung, über das Netzwerk anmelden usw.).

Berechtigungen – Windows-Berechtigungen beziehen sich darauf, was der Benutzer mit Objekten tun kann (z. B. Berechtigung zum Lesen, Schreiben, Löschen von Dateien, Verzeichnissen oder Druckern). Eine dieser Eigenschaften ist die Zugriffssteuerungsliste (ACL-Access Control List). Die ACL für ein Objekt beschreibt die speziellen Benutzer und Gruppen, denen Zugriff auf das Objekt gewährt wird, zusammen mit den entsprechenden Sicherheitsberechtigungen, die jedem Einzelnen der aufgelisteten Benutzer und Gruppen zugewiesen wurden.

Objekt (Laufwerk, Ordner oder Datei) -> Rechte Maustaste -> EIGENSCHAFTEN- > SICHERHEITSEINSTELLUNGEN (siehe Abbildung 1-1)

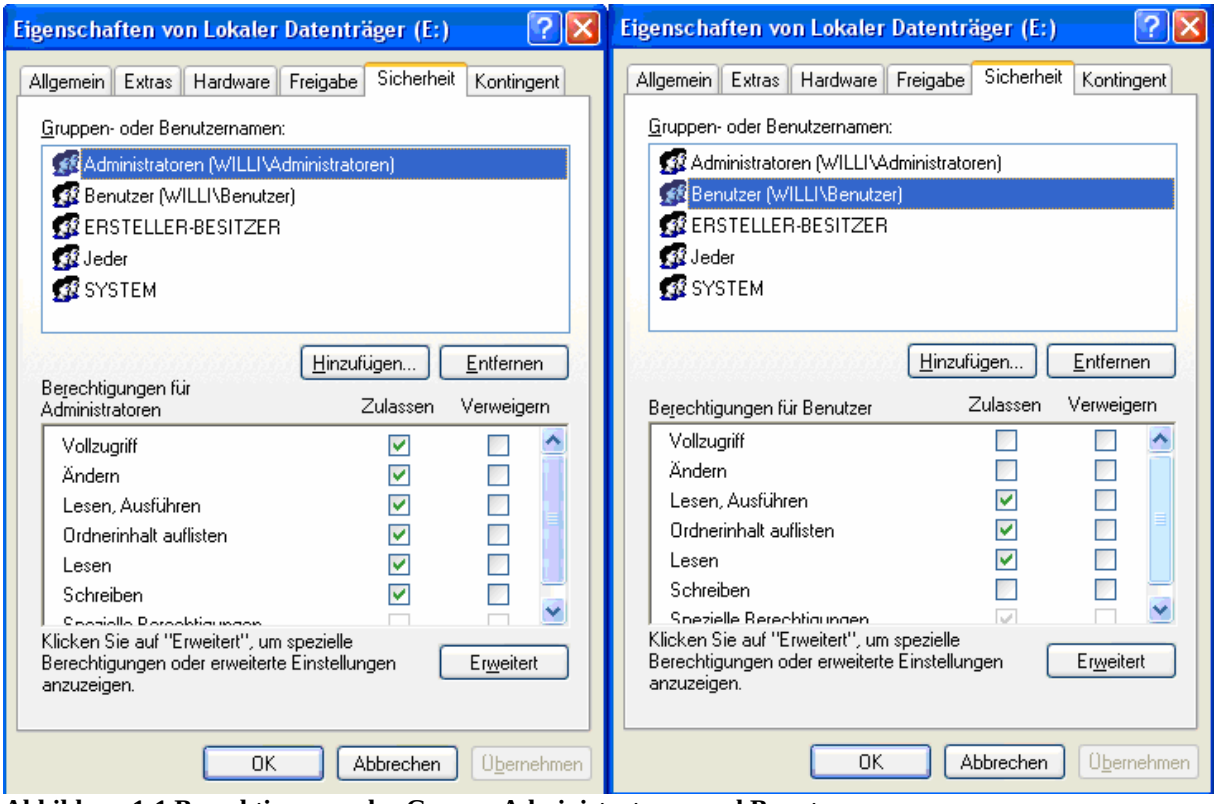


Abbildung 1-1 Berechtigungen der Gruppe Administratoren und Benutzer

Mithilfe von NTFS-Berechtigungen kann man festlegen, welche Benutzer und Gruppen Zugriff auf Dateien und Ordner erhalten und in welcher Weise die Benutzer auf den Inhalt der Dateien und Ordner zugreifen können.

2. Ordner- und Dateiberechtigungen

2.1. NTFS – Ordnerberechtigungen: (siehe Abbildung 2-1)

- **Lesen** – Anzeigen von Dateien, Unterordnern, Ordnerbesitzern, Berechtigungen und Attributen (z. B. schreibgeschützt, versteckt, Archiv und System).

- **Schreiben** – Erstellen neuer Dateien und Unterordner in einem Ordner, Ändern von Ordnerattributen, Anzeigen von Details zu Ordnerbesitz und Berechtigungen).

- **Ordnerinhalt auflisten** – Anzeigen der Namen von Dateien und Unterordnern eines Ordners.

- **Lesen und Ausführen** – Durchsuchen von Ordnern zur Suche nach anderen Dateien und Ordnern (auch wenn die Benutzer keine Zugriffberechtigungen für diese Ordner besitzen). Ausführen von Aktionen, die die Berechtigungen **Lesen** und **Ordnerinhalt auflisten** gestatten.

- **Ändern** – Löschen von Ordnern, Ausführen von Aktionen, die die Berechtigungen **Schreiben, Lesen** und **Ausführen** gestatten.

- **Vollzugriff** – Ändern von Berechtigungen, Besitzübernahme, Löschen von Unterordnern und Dateien, Ausführen von Aktionen, die alle übrigen NTFS-Ordnerberechtigungen gestatten.

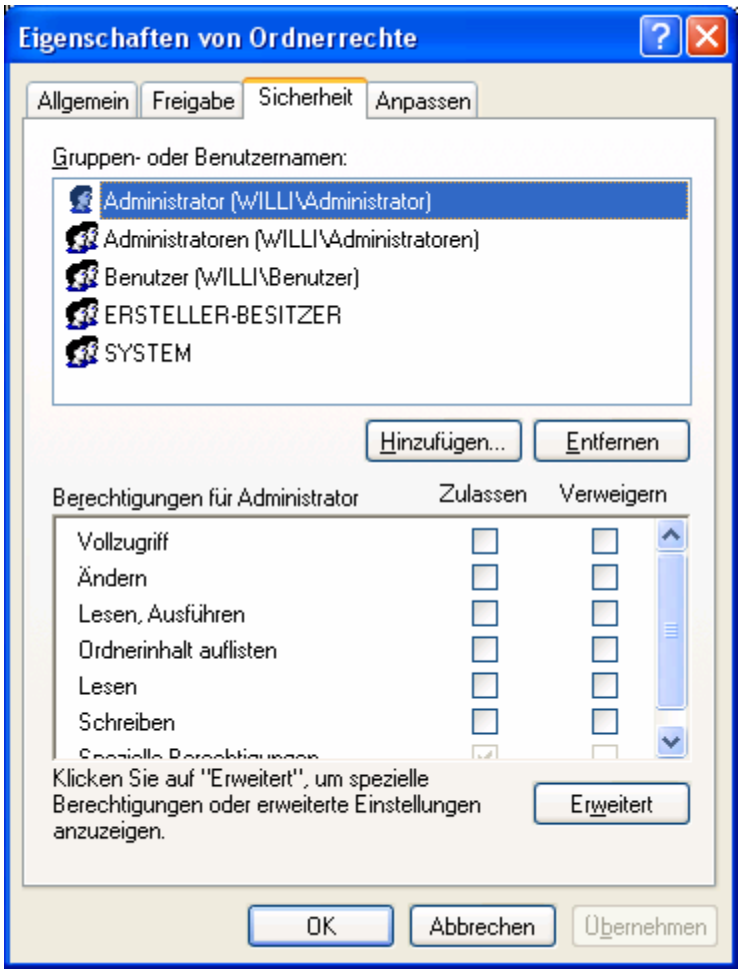


Abbildung 2-1 Ordnerberechtigungen

2.2. NTFS – Dateiberechtigungen: (siehe Abbildung 2-2)

- **Lesen** – Lesen von Dateien, Anzeigen von Dateiattributen, Besitzern und Berechtigungen.
- **Schreiben** – Überschreiben von Dateien, Ändern von Dateiattributen, Anzeigen von Dateibesitzern und Berechtigungen.
- **Lesen und Ausführen** – Ausführen von Anwendungen und allen Aktionen, die die Berechtigung **Lesen** gestattet.
- **Ändern** – Ändern und Löschen von Dateien, Ausführen von Aktionen, die die Berechtigungen **Schreiben, Lesen** und **Ausführen** gestatten.
- **Vollzugriff** - Ändern von Berechtigungen, Besitzübernahme, Ausführen von Aktionen, die alle übrigen NTFS-Ordnerberechtigungen gestatten.

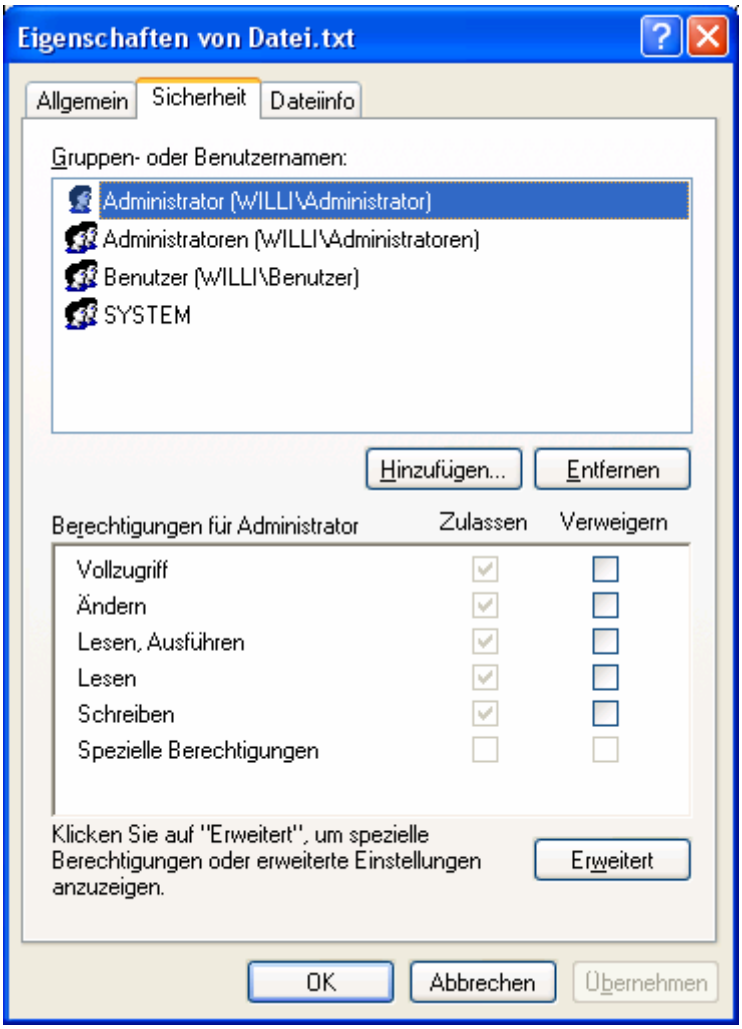


Abbildung 2-2 Dateiberechtigungen

2.3. Erweiterte Berechtigungen: (siehe Abbildung 2-3 und Abbildung 2-4)

Vollzugriff – erteilt dem Benutzer oder der Gruppe alle Berechtigungen für eine Ressource.

Ordner durchsuchen/ Datei ausführen – "Ordner durchsuchen" gestattet oder verweigert das Durchsuchen von Ordnern, um auf andere Dateien oder Ordner zuzugreifen – selbst dann, wenn der Benutzer keine Berechtigungen für den durchsuchten Ordner besitzt. "Datei ausführen" gestattet oder verweigert die Fähigkeit zum Ausführen von ausführbaren Dateien (Anwendungsdateien).

Ordner auflisten / Daten lesen – "Ordner auflisten" gilt nur für Ordner, gestattet oder verweigert die Anzeige von Datei- und Unterordnernamen innerhalb eines Ordners. "Daten lesen" gilt nur für Dateien, gestattet oder verweigert die Anzeige der Dateiinhalte.

Attribute lesen – gestattet oder verweigert die Anzeige der Datei- oder Ordnerattribute, die vom NTFS festgelegt werden.

Erweiterte Attribute lesen - gestattet oder verweigert die Anzeige der Datei- oder Ordnerattribute, die von Programmen festgelegt werden. Erweiterte Attribute werden durch Programme definiert und können sich von Programm zu Programm unterscheiden.
Dateien erstellen / Daten schreiben – Die Berechtigung **Dateien erstellen** gilt nur für Ordner und gewährt oder verweigert dem Benutzer das Recht, Dateien in dem jeweiligen Ordner zu erstellen.
Die Berechtigung **Daten schreiben** gilt nur für Dateien und gewährt oder verweigert dem Benutzer das Recht, eine Datei zu ändern und deren Inhalt zu überschreiben.

Ordner erstellen / Daten anhängen – Die Berechtigung **Ordner erstellen** gilt nur für Ordner und gewährt oder verweigert dem Benutzer das Recht, Ordner in dem jeweiligen Ordner zu erstellen.

Die Berechtigung **Daten anhängen** gilt nur für Dateien und gewährt oder verweigert dem Benutzer das Recht, Änderungen am Ende einer Datei vorzunehmen, nicht jedoch bereits existierende Inhalte zu ändern, zu löschen oder zu überschreiben.

Attribute schreiben – gestattet oder verweigert die Änderung der Datei- oder Ordnerattribute, die von NTFS festgelegt werden.

Erweiterte Attribute Schreiben – gestattet oder verweigert die Änderung der erweiterten Datei- oder Ordnerattribute. Erweiterte Attribute werden durch Programme definiert und können sich von Programm zu Programm unterscheiden.

Unterordner und Dateien löschen – gestattet und verweigert das Löschen von Unterordnern oder Dateien in einem Ordner – selbst dann, wenn für den betreffenden Unterordner oder eine jeweilige Datei nicht die Berechtigung Löschen erteilt wurde

Löschen – gestattet oder verweigert das Löschen von Dateien und Ordnern

Berechtigungen lesen – ermöglicht dem Benutzer das Lesen der für eine Datei oder einen Ordner zugewiesenen Berechtigungen

Berechtigungen ändern – ermöglicht dem Benutzer das Ändern der für eine Datei oder Ordner zugewiesenen Berechtigungen (ohne Berechtigung Vollzugriff)

Besitzrechte übernehmen – gestattet oder verweigert die Übernahme der Besitzrechte für Dateien und Ordner. Der Besitzer einer Datei kann die Berechtigungen für eine Datei oder Ordner immer Ändern, unabhängig von den für die Datei oder den Ordner festgelegten Berechtigungen

Berechtigungen für Dateien und Ordner

Spezielle Berechtigungen	Vollzugriff	Ändern	Lesen & Ausführen	Ordnerinhalt auflisten (nur Ordner)	Lesen	Schreiben
Ordner durchsuchen / Datei ausführen	x	x	x	x		
Ordner auflisten / Daten lesen	x	x	x	x	x	
Attribute lesen	x	x	x	x	x	
Erweiterte Attribute lesen	x	x	x	x	x	
Dateien erstellen / Daten schreiben	x	x				x
Ordner erstellen / Daten anhängen	x	x				x
Attribute schreiben	x	x				x
Erweiterte Attribute schreiben	x	x				x
Unterordner und Dateien löschen	x					
Löschen	x	x				
Berechtigungen lesen	x	x	x	x	x	x
Berechtigungen ändern	x					
Besitz übernehmen	x					

Abbildung 2-3 Erweiterte Berechtigungen I

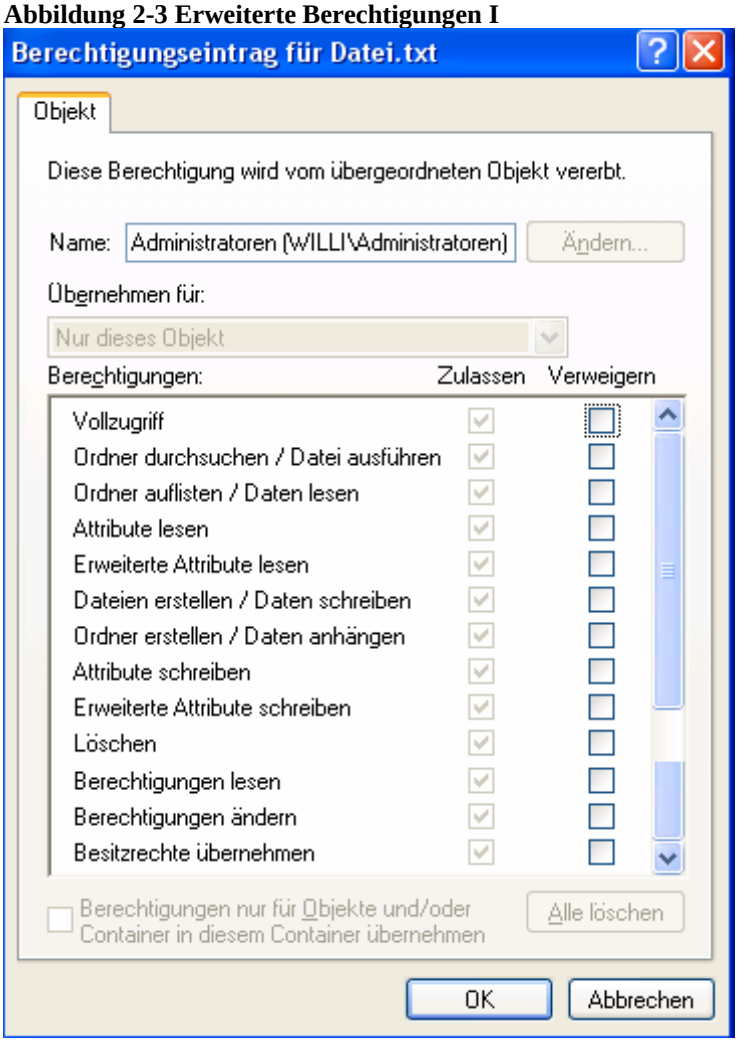


Abbildung 2-4 Erweiterte Berechtigungen II

3. Hierarchie der Berechtigungen

Berechtigungen werden standardmäßig von Ordnern auf Dateien und Unterordner übertragen (vererbt).

3.1. Explizite Berechtigungen – werden direkt an ein Objekt oder eine Organisationseinheit gebunden: (siehe Abbildung 3-1).

3.2. Vererbte Berechtigungen – werden von einem übergeordneten auf ein untergeordnetes Objekt weitervererbt: (siehe Abbildung 3-2).

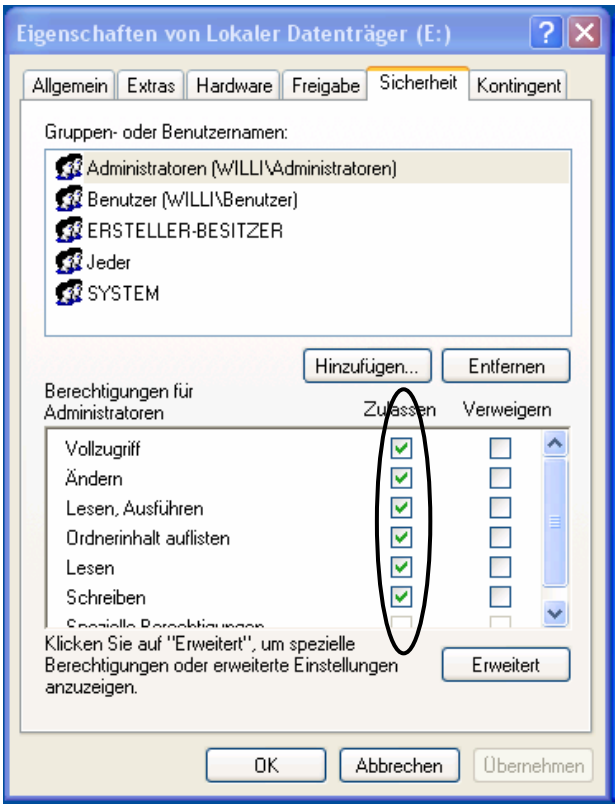


Abbildung 3-1 Explizite Berechtigungen

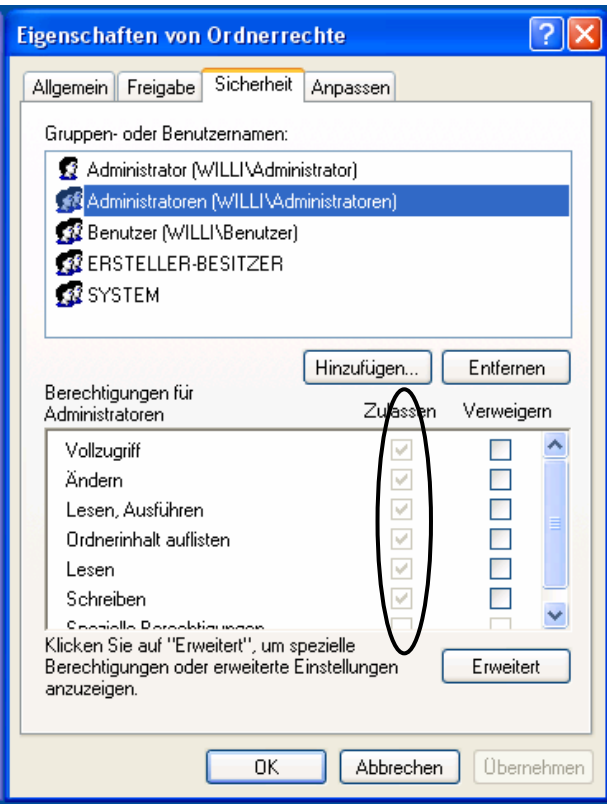


Abbildung 3-2 Vererbte Berechtigungen

3.3. Effektive Berechtigungen – die effektiven Berechtigungen eines Benutzers für eine bestimmte Ressource setzen sich aus der Summe der NTFS-Berechtigungen zusammen, die Sie einem einzelnen Benutzerkonto auf allen Gruppen gewähren, denen der Benutzer angehört: (siehe Abbildung 3-3 und Abbildung 3-4)

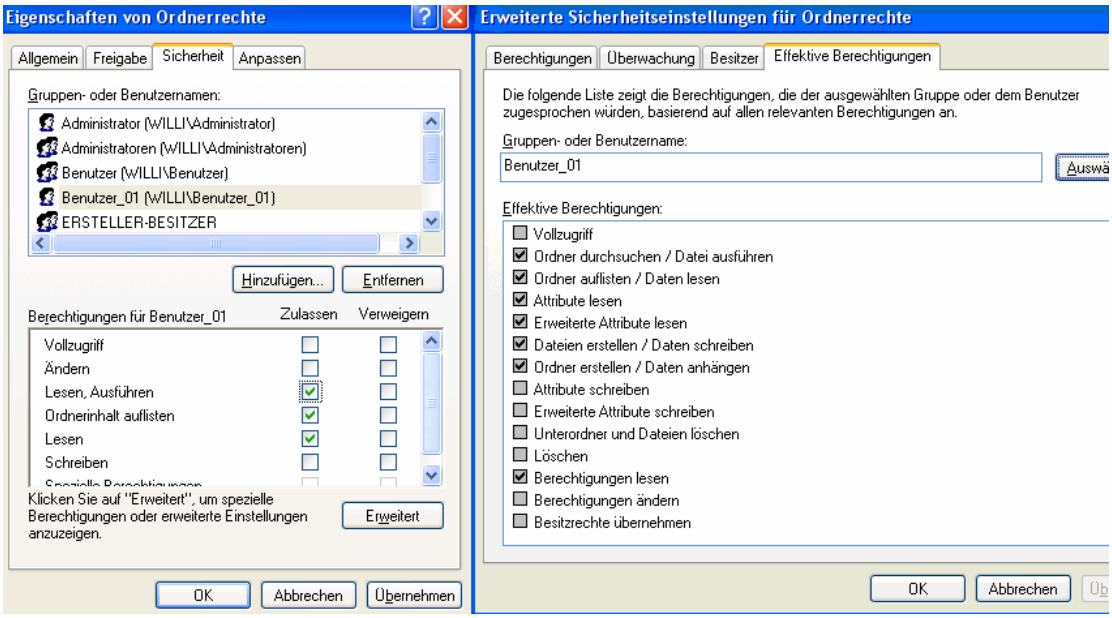


Abbildung 3-3 Berechtigungen des Benutzers Benutzer_01 auf einen Ordner mit dem Namen Ordnerrechte

Wenn ein Benutzer, z.B. Benutzer_01, die Leseberechtigung für einen Ordner besitzt (siehe Abbildung 3-3) und Benutzer_01 Mitglied einer Gruppe (z. B. Testbenutzer) mit Schreibberechtigung für denselben Ordner ist, besitzt der Benutzer die Berechtigung Lesen und Schreiben für diesen Ordner. (siehe Abbildung 3-4)

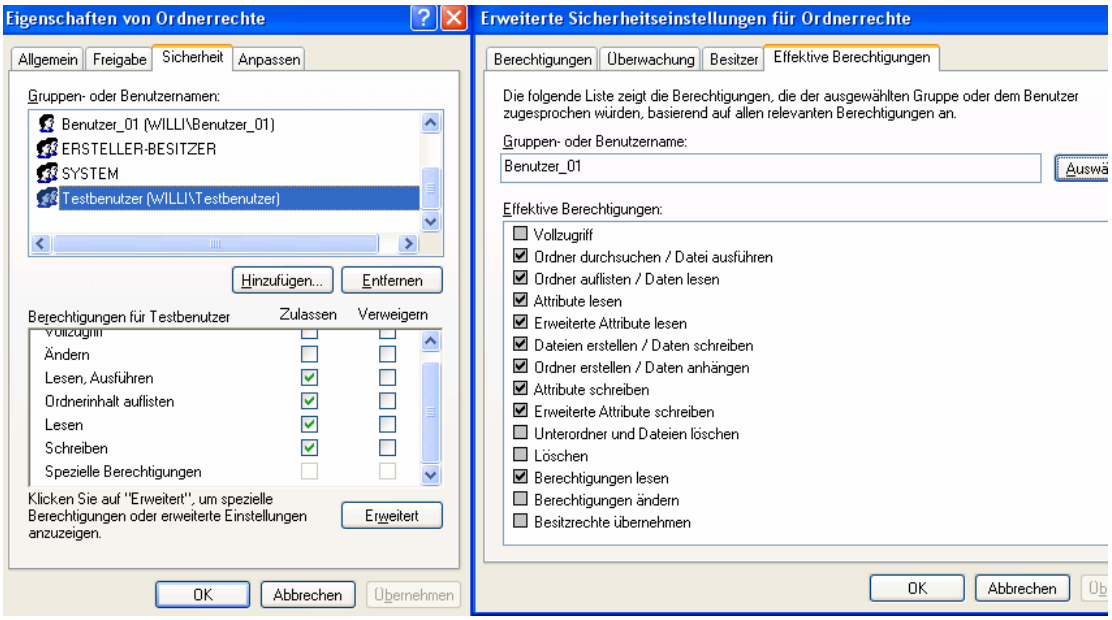


Abbildung 3-4 Berechtigungen der Gruppe Testbenutzer und des Benutzers_01

3.4. Deaktivieren der Berechtigungsvererbung:

Standardmäßig ist die Einstellung **Berechtigungen für übergeordnete Objekte auf untergeordnete Objekte, sofern anwendbar, vererben** aktiviert. (siehe Abbildung 3-5)

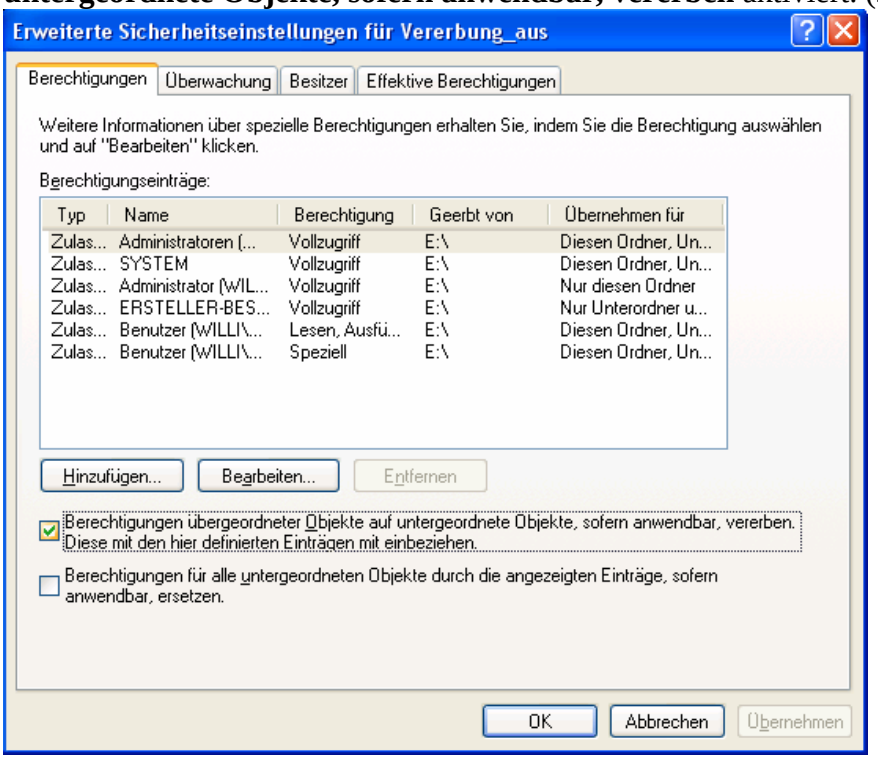


Abbildung 3-5 Vererbung aktiviert

Durch Deaktivierung des Kontrollkästchen „Berechtigungen übergeordneter Objekte … vererben…“ kann man die Berechtigungsvererbung unterbrechen. Es stehen folgende Optionen zur Verfügung: (siehe Abbildung 3-6)

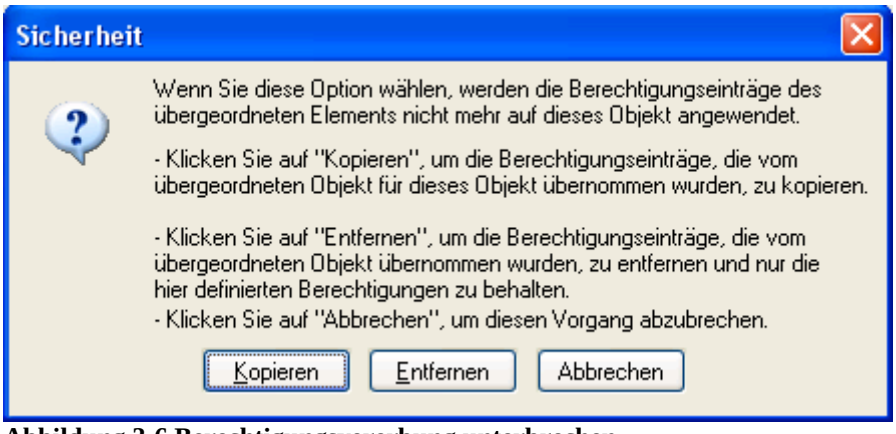


Abbildung 3-6 Berechtigungsvererbung unterbrechen

Kopieren – kopiert die zuvor vom übergeordneten Objekt vererbten Berechtigungseinträge für das untergeordnete Objekt und sorgt dafür, dass später erteilte Berechtigungen nicht mehr durch den übergeordneten Ordner vererbt werden. (siehe Abbildung 3-7, Mitte)

Entfernen – Entfernt die zuvor vom übergeordneten Objekt vererbten Berechtigungseinträge für das untergeordnete Objekt und weist dem untergeordneten Objekt nur explizit zugewiesene Berechtigungen zu. (siehe Abbildung 3-7, Rechts)

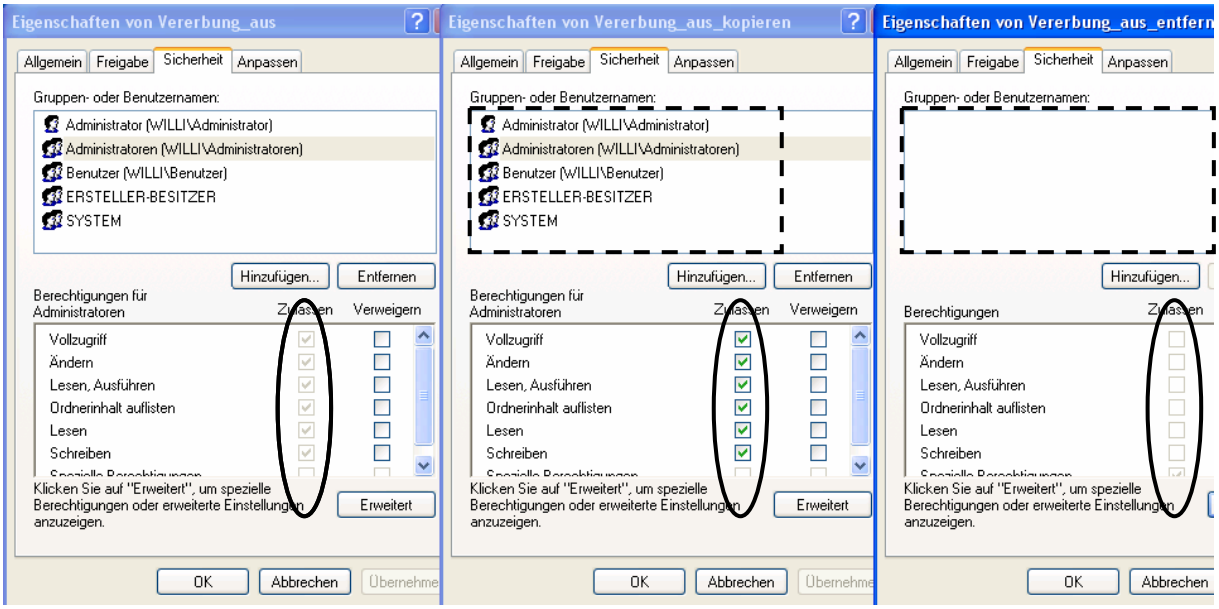


Abbildung 3-7 Berechtigungen – vererbt (Links), kopiert (Mitte), entfernt (Rechts)

Abbrechen – schließt das Dialogfeld Sicherheit.

3.5. Außerkraftsetzung von Ordnerberechtigung durch Dateiberechtigungen:

NTFS-Dateiberechtigungen haben Vorrang vor NTFS-Ordnerberechtigungen.
Sie können den Zugriff auf eine Bestimmte Datei für ein Benutzerkonto oder eine Gruppe explizit setzen. Z. B. ein Benutzer hat auf einen Ordner die Berechtigung Schreiben, aber auf die Datei nur Berechtigung lesen. Der Benutzer kann diese Datei nur lesen. (siehe Abbildung 3-8).

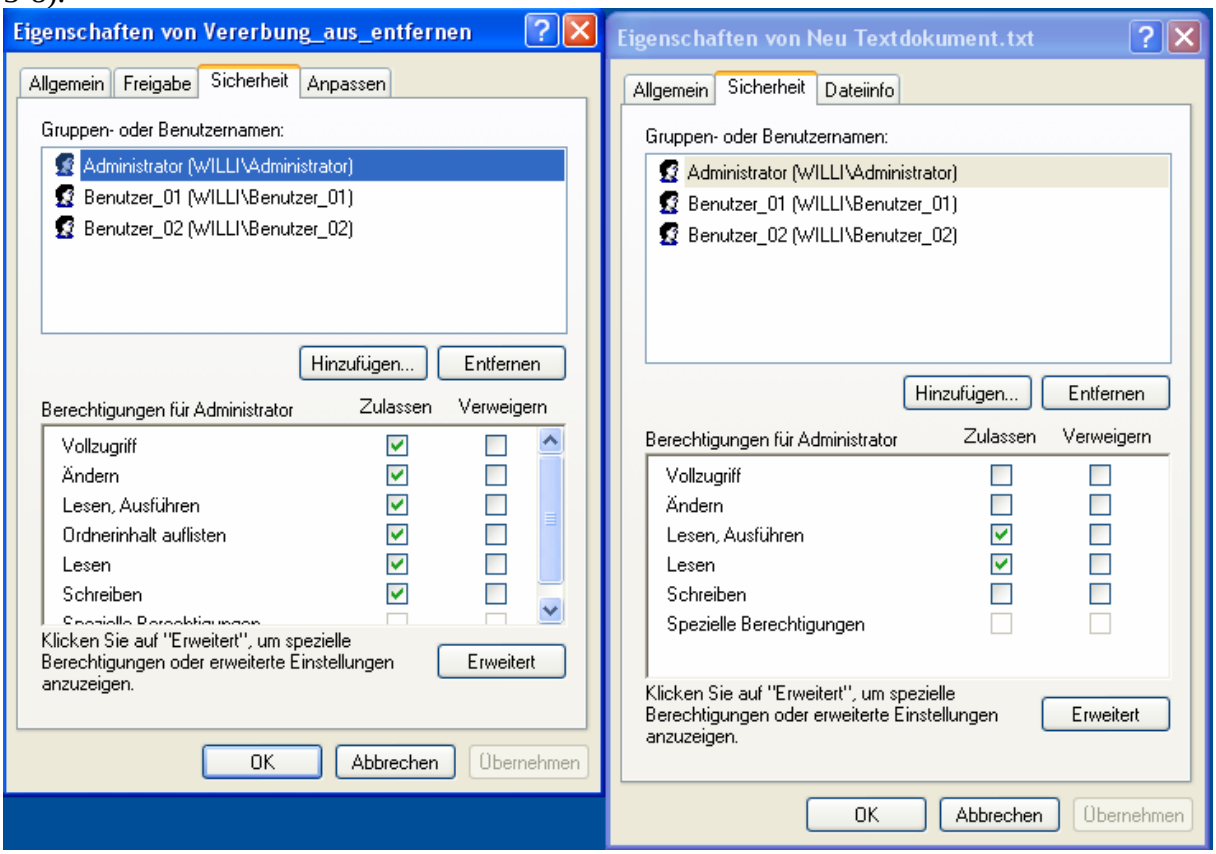


Abbildung 3-8 Dateiberechtigungen setzen Ordnerberechtigungen außer Kraft

3.6. Außerkraftsetzung von Berechtigungen durch eine Berechtigungsverweigerung:

Man kann den Zugriff auf eine bestimmte Datei für ein Benutzerkonto oder eine Gruppe explizit verweigern. Die Verweigerung einer Berechtigung setzt jegliche Zuweisungen dieser Berechtigung an anderer Stelle außer Kraft. (siehe Abbildung 3-9)

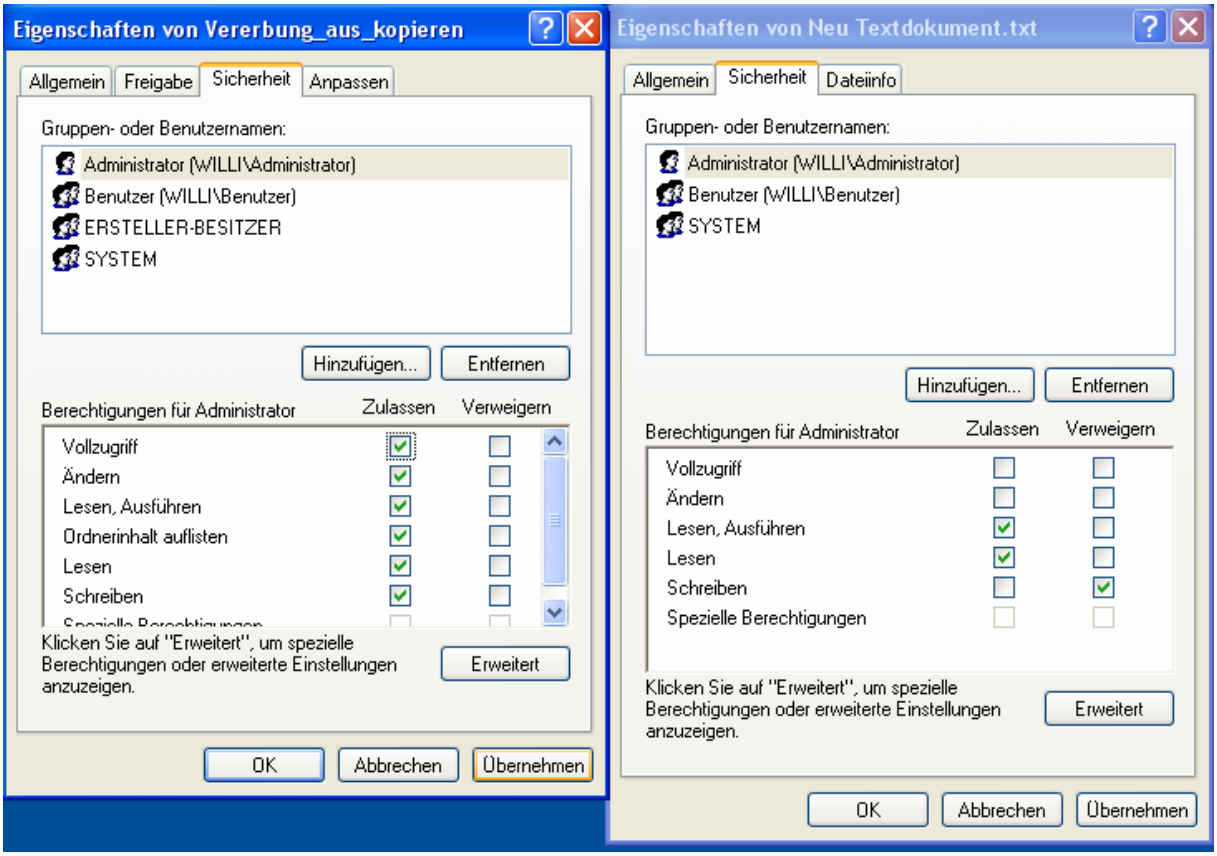


Abbildung 3-9 Außerkraftsetzung von Berechtigungen durch eine Berechtigungsverweigerung

Es gilt:

NTFS-Berechtigungen sind kumulativ.
Dateiberechtigungen überschreiben Ordnerberechtigungen.
Eine Zugriffsverweigerung setzt anderweitig erteilte Berechtigungen außer Kraft.

4. Kopieren von Dateien und Ordnern

4.1. Kopieren einer Datei innerhalb eines NTFS-Volumes oder zwischen zwei NTFS-Volumes: (siehe Abbildung 4-1)

Für das Kopieren einer Datei innerhalb eines NTFS-Volumes oder zwischen zwei NTFS-Volumes gelten folgende Regeln: (siehe Abbildung 4.1)

- Windows XP Professional betrachtet die Datei als neue Datei. Als neue Datei übernimmt die Datei die Berechtigungen des Zielordners. Der Benutzer, der den Kopiervorgang durchgeführt hat, hat Vollzugriff auf die Datei.
- Man muss für den Zielordner über die Berechtigung **Schreiben** verfügen, um Dateien und Ordner in den Zielordner kopieren zu können.
- Man wird standardmäßig zum Ersteller und Besitzer der kopierten Datei oder des Ordners.

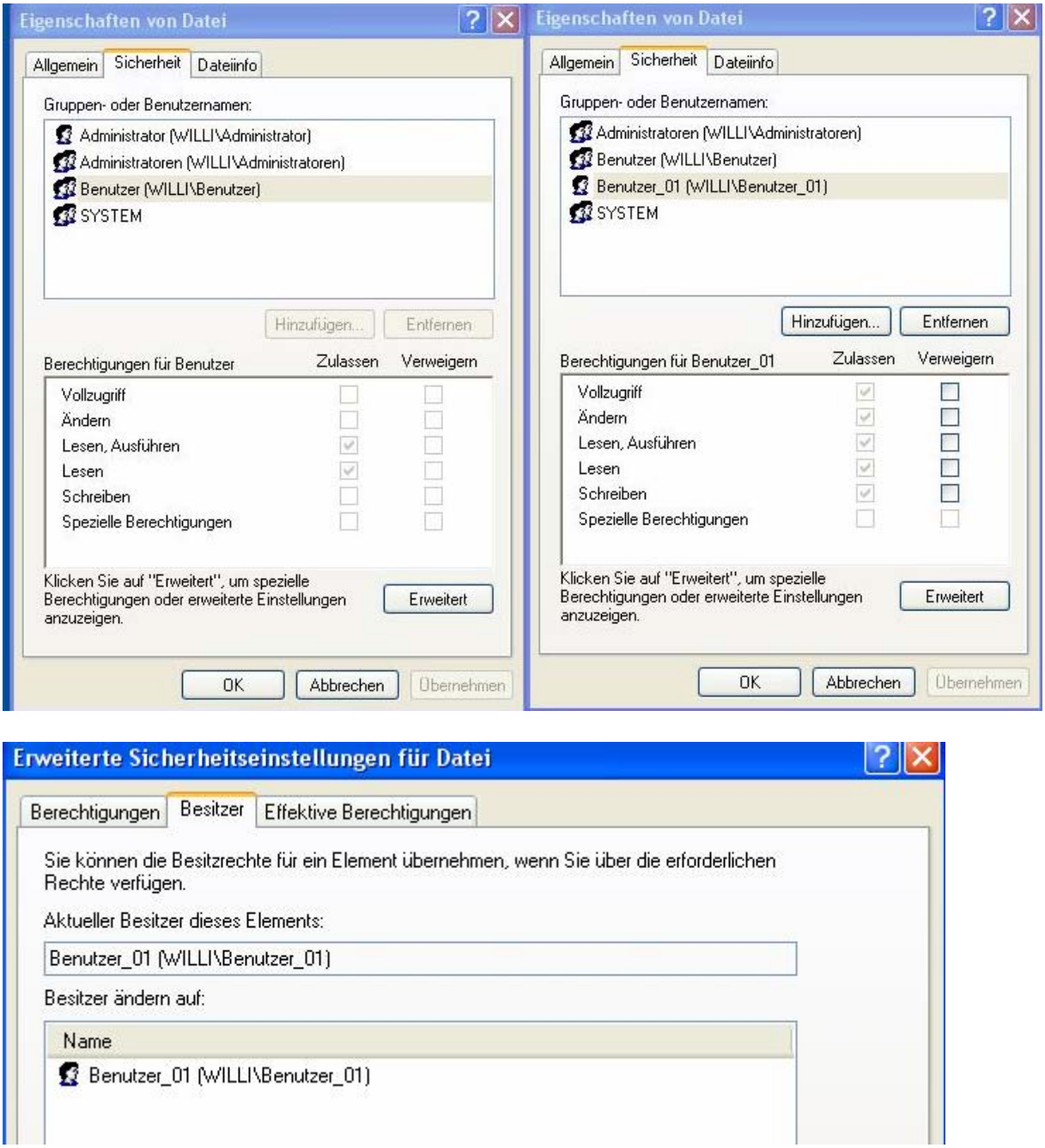


Abbildung 4-1 Kopieren einer Datei innerhalb eines NTFS-Volumes oder zwischen zwei NTFS-Volumes

5. Verschieben von Dateien und Ordnern

5.1. Verschieben innerhalb eines NTFS-Volumes: (siehe Abbildung 5-1)

- Die Datei bzw. der Ordner behält seine ursprünglichen Berechtigungen und Besitzer.
- Man muss für den Zielordner über die Berechtigung **Schreiben** verfügen, um Dateien und Ordner in den Zielordner verschieben zu können.
- Man muss für die Quelldatei oder den Quellordner über die Berechtigung **Ändern** verfügen.
- Die Datei bzw. der Ordner wird aus dem Quellordner gelöscht, nachdem diese(r) in den Zielordner kopiert wurde.

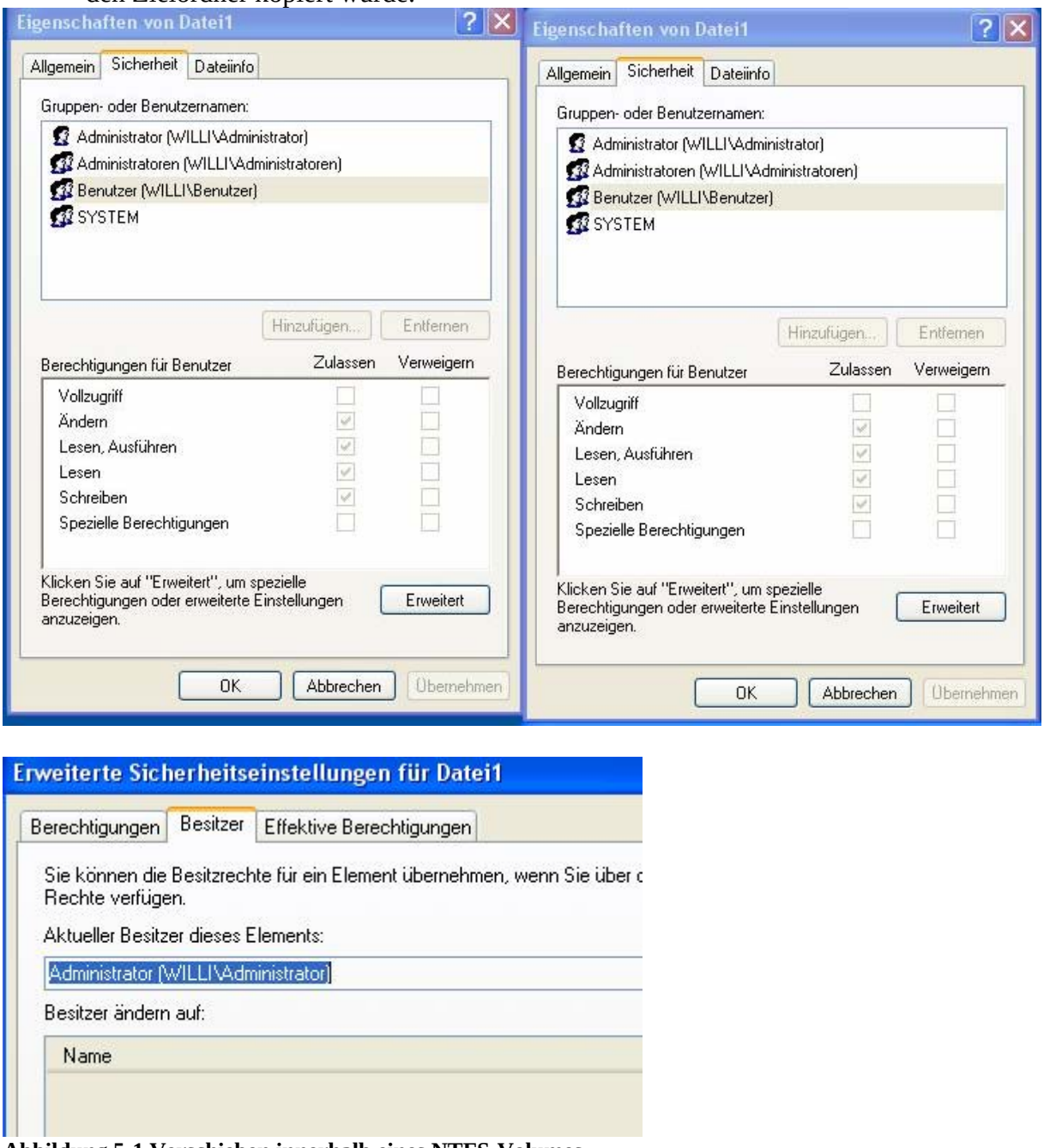


Abbildung 5-1 Verschieben innerhalb eines NTFS-Volumes

5.2. Verschieben zwischen zwei NTFS-Volumes: (siehe Abbildung 5-2)

- Datei oder Ordner erben die Berechtigungen des Zielordners
- Man muss für den Zielordner über die Berechtigung **Schreiben** verfügen, um Dateien und Ordner in den Zielordner verschieben zu können.
- Man muss für die Quelldatei oder den Quellordner über die Berechtigung **Ändern** verfügen.
- Die Datei bzw. der Ordner wird aus dem Quellordner gelöscht, nachdem diese(r) in den Zielordner kopiert wurde.
- Man wird zum Ersteller und Besitzer der kopierten Datei oder des Ordners

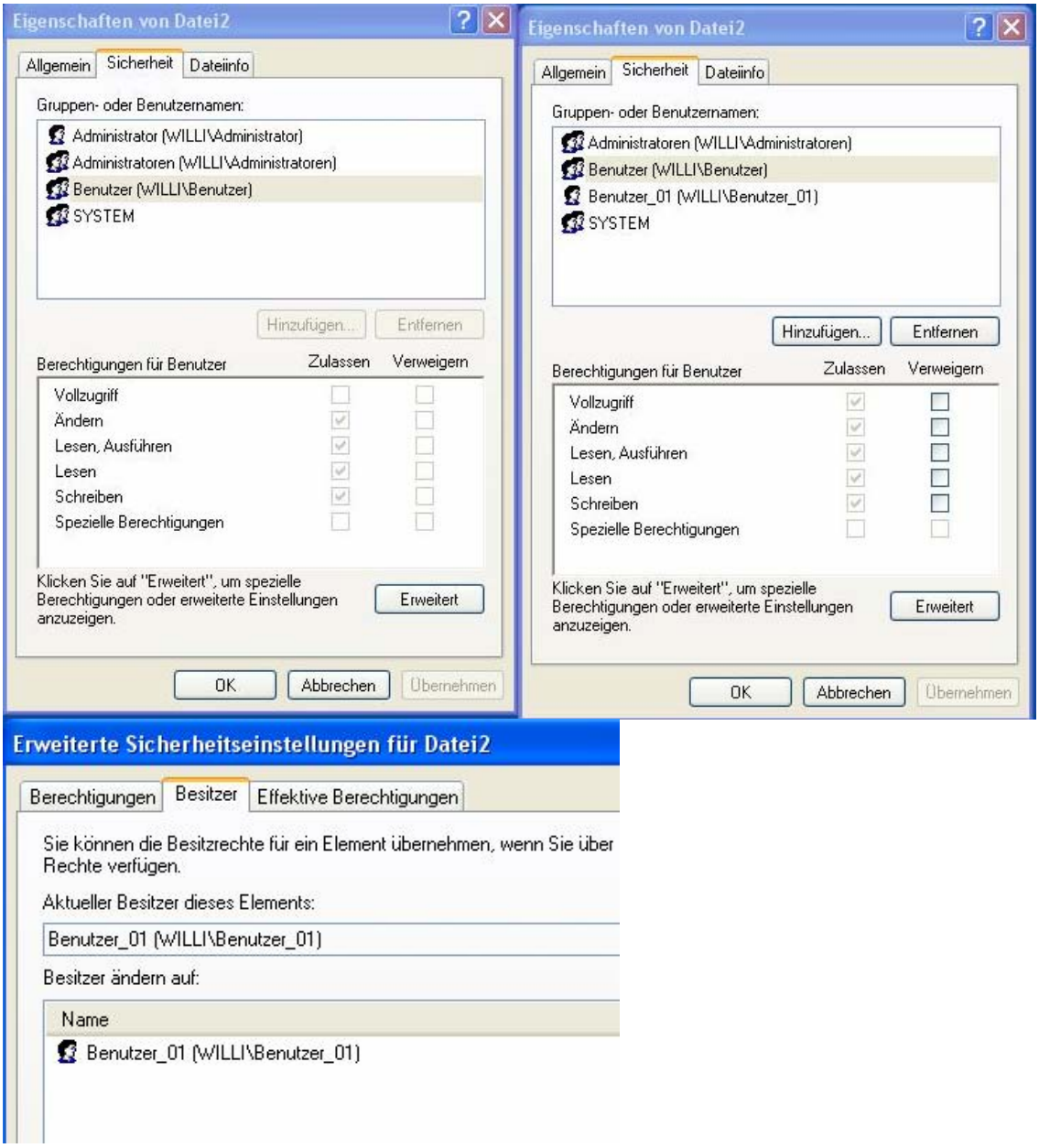


Abbildung 5-2 Verschieben zwischen zwei NTFS-Volumes

Wenn man Dateien oder Ordner auf ein FAT-Volume verschiebt, verlieren die Dateien und Ordner ihre NTFS-Berechtigungen.

6. Besitzer für Dateien und Ordner

Jedes Objekt auf einem NTFS-Volume verfügt über einen Besitzer (siehe Abbildung 6-1). Dieser legt die Vergabe von Berechtigungen für das Objekt fest. Besitzrechte können von einem Benutzerkonto auf ein anderes übertragen werden. Um den Besitz zu übernehmen, muss man über die Berechtigung „Besitzrechte übernehmen“ oder „Vollzugriff“ verfügen.

- Der Besitzer (oder ein Benutzer mit der Berechtigung Vollzugriff) kann einem Benutzerkonto oder einer Gruppe die Standardberechtigung "Vollzugriff" oder die spezielle Berechtigung „Besitzrechte übernehmen“ erteilen. Damit ist das Benutzerkonto oder ein Mitglied der betreffenden Gruppe berechtigt, die Besitzrechte zu übernehmen.

- Ein Administrator hat grundsätzlich die Möglichkeit, den Besitz für einen Ordner oder eine Datei zu übernehmen, unabhängig von den zugewiesenen Berechtigungen.

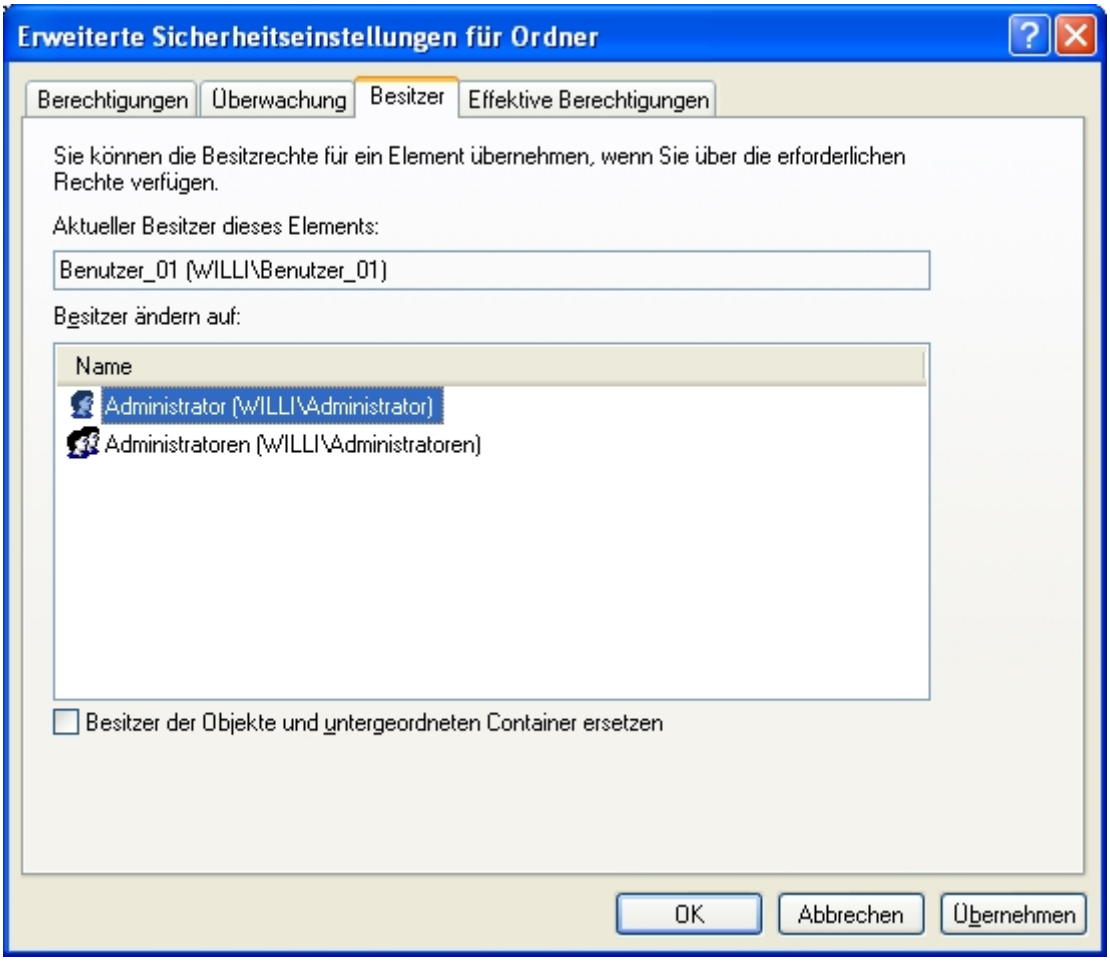


Abbildung 6-1 Besitzer unter Windows XP

Unter Windows XP ist es nicht möglich, einem Benutzer die Besitzrechte für eine Datei oder einen Ordner zuzuweisen. Dies geht nur bei einem Server Betriebssystem wie Windows Server 2003 (siehe Abbildung 6-2)

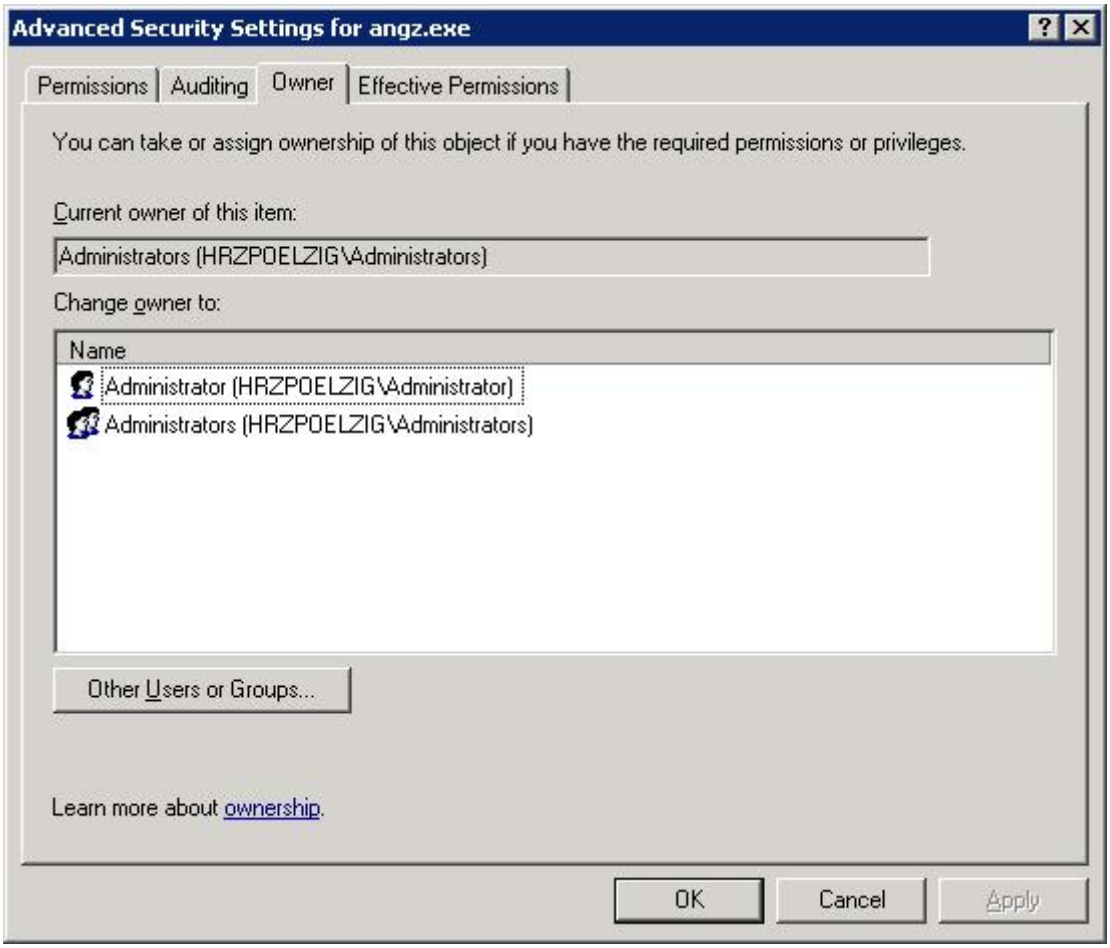


Abbildung 6-2 Besitzer unter Server 2003

7. Verwalten freigegebener Ordner

Durch den Einsatz von freigegebenen Ordnern können Sie Benutzern über das Netzwerk den Zugriff auf Ressourcen (Drucker, Ordner und Dateien) ermöglichen. Nach der Freigabe einer Ressource über das Netzwerk können die Benutzer sich die Ressource über das Netzwerk verfügbar machen und damit arbeiten.

7.1. Voraussetzungen

- Unter Windows XP Professional können die Mitglieder der vordefinierten Gruppe **Administratoren** und **Hauptbenutzer** Ordner freigeben (in der Domäne sind es die die Gruppen **Administratoren** und **Server-Operatoren** die Ordner freigeben können – **Hauptbenutzer** ist eine lokale Gruppe und nicht auf einem Domaincontroller verfügbar).
- Die **„Datei- und Druckerfreigabe“** in den Eigenschaften der Netzwerkverbindung muss **aktiviert** sein.
- In der **Firewall** unter Windows XP muss unter „Ausnahmen“ die „Datei- und Druckerfreigabe“ eingetragen sein, damit die entsprechenden Ports offen sind.
- Die **einfache Dateifreigabe** muss **deaktiviert** sein (Windows Explorer → Extras → Ordneroptionen → Ansicht).
- Der Benutzeraccount muss über ein **Passwort** verfügen, um auf eine Netzwerkfreigabe zugreifen zu können (siehe Abbildung 7-1).

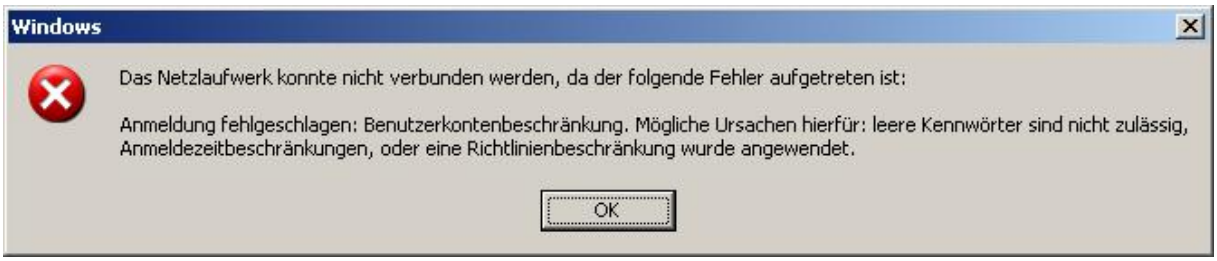


Abbildung 7-1 Netzlaufwerk verbinden ohne Passwort

- Um auf die Netzwerkressource zugreifen zu können, muss der Benutzer **sowohl** über entsprechende **Berechtigungen für den freigegebenen Ordner** verfügen (Registerkarte „Freigabe“ → Berechtigungen [siehe Abbildung 7-2]) **als auch** die entsprechenden **NTFS Berechtigungen** (Registerkarte „Sicherheit“) besitzen.

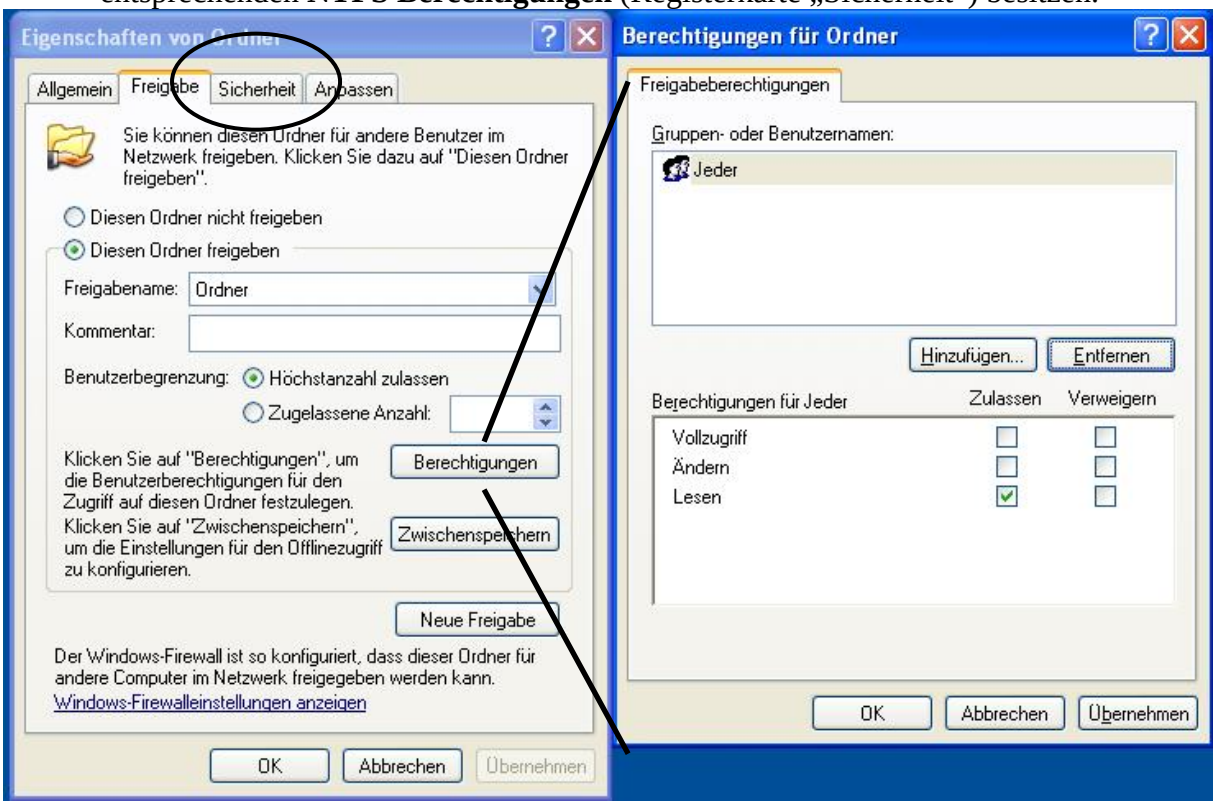


Abbildung 7-2 Netzwerkfreigabe

- Die standardmäßig erteilte Berechtigung für einen freigegeben Ordner lautet **Lesen** (ab XP mit SP1). Diese Berechtigung wird bei Freigabe eines Ordners der Gruppe **Jeder** zugewiesen.
- Die **Berechtigungen** für freigegebene Ordner **gelten für den gesamten Ordner**, nicht für einzelne Dateien.
- Über die Berechtigungen für freigegebene Ordner kann der Zugriff auf diese Ordner nicht für Benutzer eingeschränkt werden, die lokal an dem Computer arbeiten. Die **Berechtigungen für freigegebene Ordner gelten nur für Benutzer, die über das Netzwerk** auf den freigegebenen Ordner **zugreifen**.

7.2. Freigeben eines Ordners

Mit rechter Maustaste auf den Ordner klicken → Eigenschaften → Freigabe (siehe Abbildung 7-3)

Diesen Ordner (nicht) freigeben: Bestimmt, ob der Ordner für das Netzwerk freigegeben wird. Wenn eine Freigabe aufgehoben werden soll, diesen Punkt anklicken.

Freigabename: Der Name der Freigabe die beim Mounten angegeben werden muss. Kann beliebig gewählt werden und muss nicht mit dem Ordnernamen übereinstimmen.

Kommentar: Wird beim Browsen über die Netzwerkumgebung als Kommentar angezeigt.

Benutzerbegrenzung (die Anzahl der Benutzer, die gleichzeitig eine Verbindung zum freigegeben Ordner herstellen können. (Max. 10 bei Workstation), lässt man normalerweise leer.

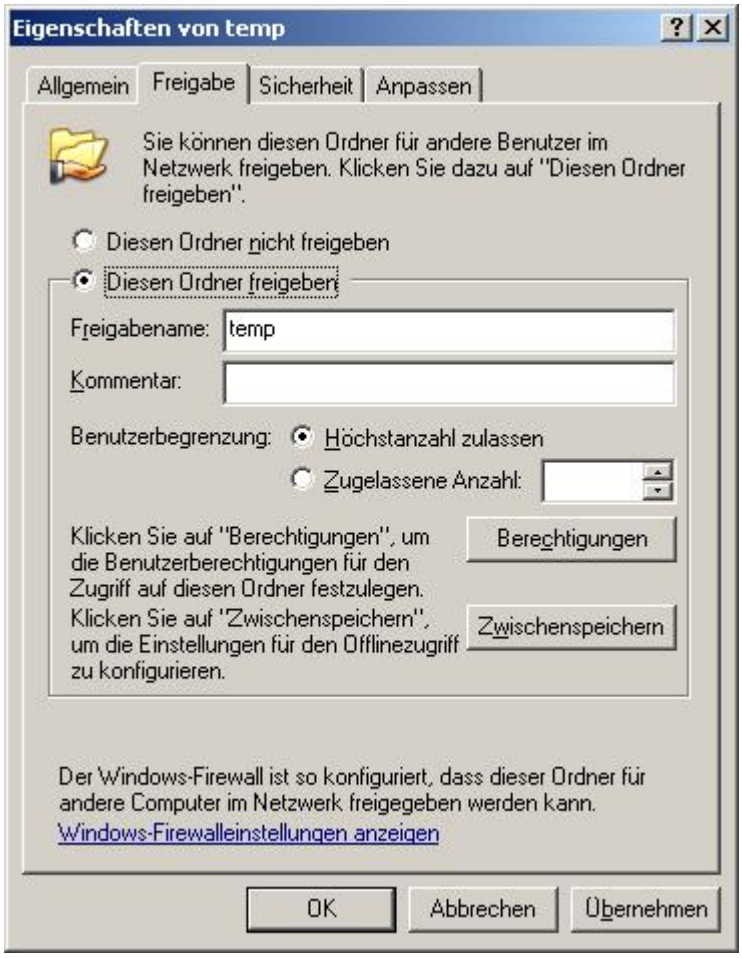


Abbildung 7-3 Freigabe

Neue Freigabe- In bestimmten Situationen ist es u. U. erforderlich, für einen freigegebenen Ordner unterschiedliche Berechtigungen festzulegen. In diesen Fällen können Sie mehrere Freigabenamen für einen freigegebenen Ordner erstellen und diesen unterschiedliche Berechtigungen zuweisen. Der Button erscheint erst, sobald schon eine Freigabe auf dem Ordner existiert.

- Berechtigungen für freigegebene Ordner:
  Lesen – Anzeigen von Ordnernamen, Dateinamen, Datendateien und Attribute; Ausführen von Programmdateien; Ändern von Ordnern im freigegebenen Ordner

  Ändern – Erstellen von Ordnern, Hinzufügen von Dateien zu Ordnern, Ändern von Daten in Dateien, Anhängen von Daten an Dateien, Ändern von Dateiattributen, Löschen von Ordnern und Dateien; Ausführen von Aktionen, die über die Berechtigungen **Lesen** gestattet werden.

  Vollzugriff – Ändern von Dateiberechtigungen, Übernehmen der Besitzrechte für Dateien; Ausführen von Aktionen, die über die Berechtigungen **Ändern** gestattet werden.

7.3. Verbindungsherstellung zu einem freigegebenen Ordner

Allgemeine Informationen zum Verbinden eines Netzlaufwerkes

Zum Mounten (Mounten = Verbinden einer entfernten Netzwerkressource über das Netzwerk an den lokalen Rechner) eines im Netzwerk freigegebenen Ordners benötigt man:

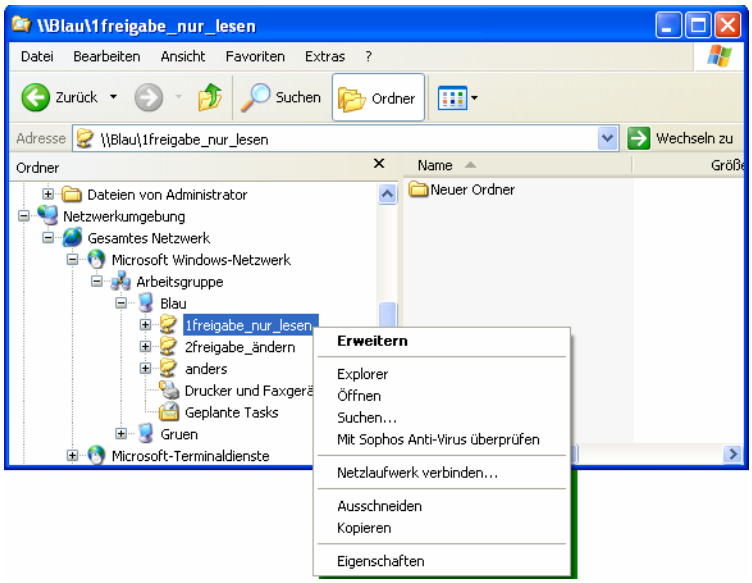
1. Den **Namen des Rechners**, auf dem der freigegebene Ordner liegt.
2. Den genauen **Namen der Freigabe**, unter welcher der Ordner für das Netzwerk freigegeben wurde.
3. **Nutzernamen und Passwort** eines Benutzers auf dem Computer, welcher den freigegebenen Ordner enthält.
4. Korrekt gesetzte Rechte und Berechtigungen, um Zugriff auf die Dateifreigabe zu erhalten.

„Servername“ wird im Folgenden als Name des Rechners verwendet, welcher den freigegebenen Ordner enthält. Gemeint ist der vollqualifizierte Rechnername (FQDN = Fully Qualified Domain Name) des Computers wie z.B. www.rz.uni-frankfurt.de.
Sicher funktionieren sollten beim Mounten immer der FQDN sowie die IP-Adresse des Rechners/Servers. Oft reicht auch nur die Angabe des Netbios-Namens. Sollte es mit dem Mounten über Angabe des Netbios Namens nicht funktionieren, immer FQDN bzw. direkt die IP-Adresse des Rechners zum Verbinden benutzen.
Im Problemfall testweise den Server anpingen mit DNS Namen bzw. IP-Adresse (! evtl. blockt eine Firewall die Pings).
Beispiel:

FQDN („DNS Name“):	www.rz.uni-frankfurt.de
IP Adresse:	141.2.22.39
Netbios Name (veraltet):	www

„Für Faule“: Mounten durch „browsen“ in der Netzwerkumgebung

- Starten Sie den Explorer und klicken Sie sich zu dem freigegebenen Ordner durch (Netzwerkumgebung → Gesamtes Netzwerk → Microsoft Windows Netzwerk → Name der Domain/Arbeitsgruppe → Name des Computers → rechter Mausklick auf die Freigabe → Netzlaufwerk verbinden → Laufwerksbuchstabe auswählen



„Standardverfahren“: Mounten über den Explorer (Extras → Netzlaufwerk verbinden)

- Über Arbeitsplatz → Extras → Netzlaufwerk verbinden (siehe Abbildung 7-4)
  - Dasselbe Ergebnis wie mit dem net use Kommando
  - Vorteil: einfach zu bedienen durch grafische Oberfläche, schnelles Verbinden einzelner Laufwerke möglich, Nachteil: ungeeignet für das Mounten vieler Freigaben (dauert zu lang).

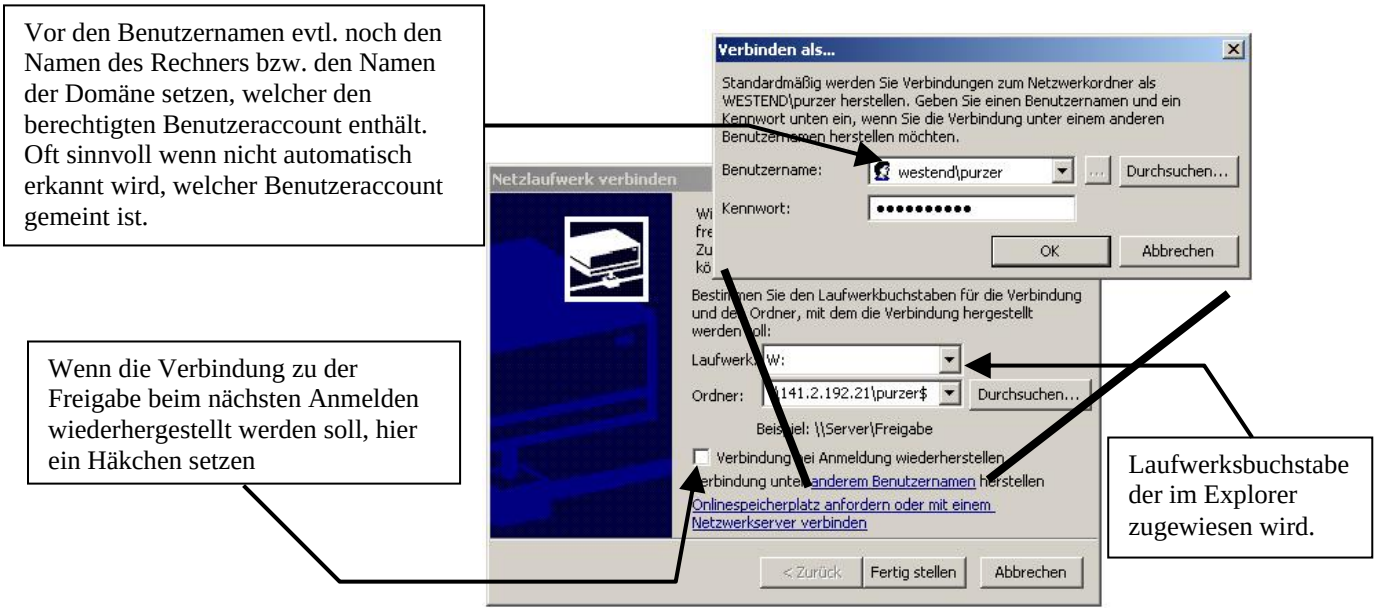


Abbildung 7-4 Mounten mit Laufwerksbuchstaben II

„Für Profis“: Mounten über Kommandozeile und dem „net use“ Befehl

- An der Eingabeaufforderung (Start → ausführen → cmd) das Kommando net use benutzen. Hilfe zu net use mit dem Kommando net use /?
  Beispiel: net use u: \\servername\freigabename
  - Ergebnis: Das Netzlaufwerk wird mit dem Buchstaben U:\ im Explorer gemountet
  - Vorteil: gut beim Arbeiten mit batch-Dateien, „mächtige“ Kommandozeile, Nachteil: „fummelig, dauert meist länger“

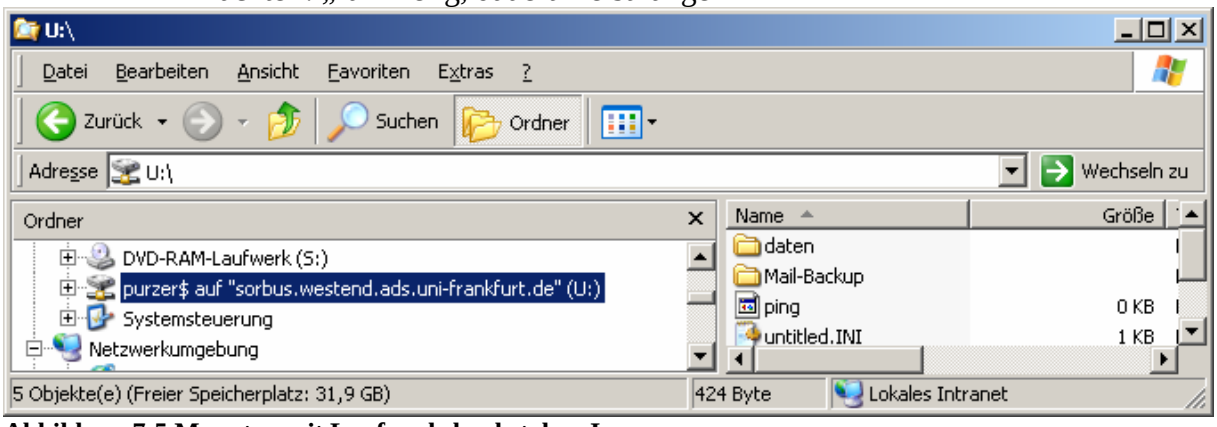


Abbildung 7-5 Mounten mit Laufwerksbuchstaben I

„… nur mal schnell“: Mounten über UNC ohne Laufwerksbuchstaben

- Eingabe eines Pfades gemäß Universal Naming Convention (UNC) in dem Dialog Start -> Ausführen mit dem Format \\Servername\Freigabename
  - Ergebnis: Ein neues Fenster wird geöffnet mit dem Inhalt des gemounteten Ordners. Es wird **kein Laufwerksbuchstabe im Explorer** angelegt.
  - Vorteil: geht schnell, Nachteil: wenn man das Fenster schließt ist das Netzlaufwerk nicht mehr verbunden.



Abbildung 7-6 Ohne Laufwerksbuchstaben mounten

„Für Esoteriker“: Mounten „unterhalb“ der Netzwerkumgebung

- Die Netzwerkumgebung öffnen. Dort den Assistenten starten über „Netzwerkressource hinzufügen“ und die entsprechenden Daten (Servername\Freigabename) hinzufügen.
  - Ergebnis: Die Freigabe wird unter dem Symbol „Netzwerkumgebung“ eingebunden.

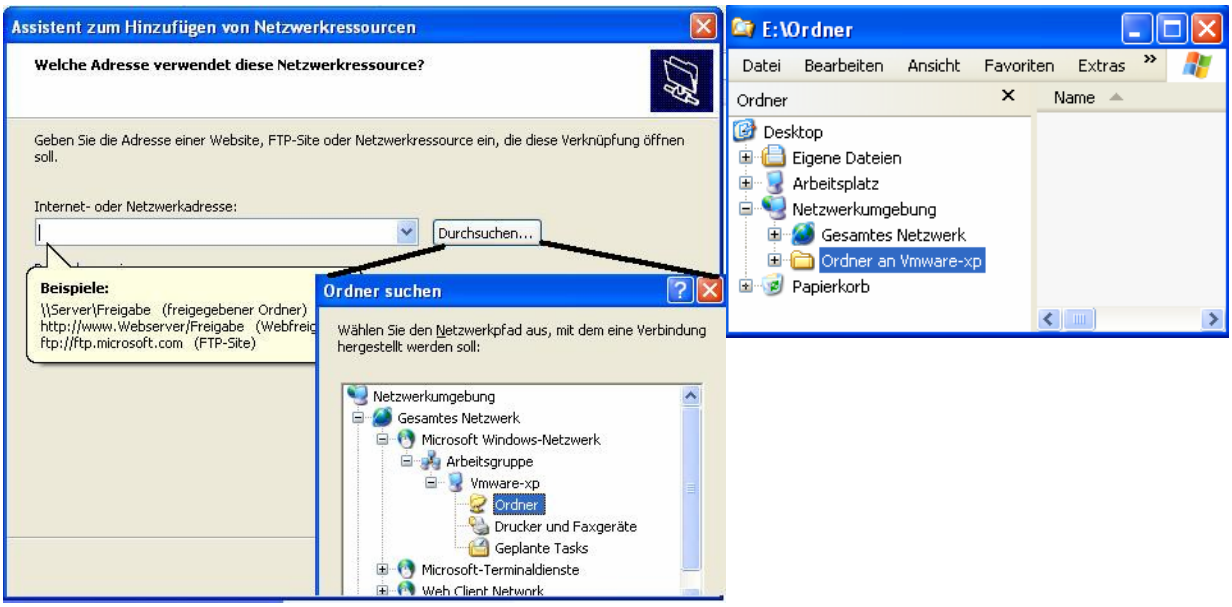


Abbildung 7-7 Mounten in Netzwerkumgebung

7.4. Administrative Ordnerfreigaben

Windows XP gibt verschiedene Ordner zu Verwaltungszwecken automatisch frei.
Diese Freigaben sind mit einem Dollarzeichen ($) gekennzeichnet, wodurch die Freigaben ausgeblendet werden, wenn ein Benutzer einen Computer durchsucht (sog. versteckte Freigaben).
C$, D$, E$ usw. - Das Stammverzeichnis aller Volumes (=Festplatten) wird standardmäßig freigegeben. Windows XP weist der Gruppe **Administratoren** für diese Freigaben die Berechtigung **Vollzugriff** zu.

Admin$ - Der Systemstammordner (C:\WINDOWS), Windows XP weist der Gruppe **Administratoren** für diese Freigabe die Berechtigung **Vollzugriff** zu.

IPC$ - Inter-Process-Communication (IPC). Eine Ressource, die zum Freigeben der "Named Pipes" dient, die für die Kommunikation zwischen Programmen unerlässlich sind. IPC$ wird während der Remoteverwaltung eines Computers und zum Anzeigen der auf einem Computer freigegebenen Ressourcen verwendet.

Print$ - Bei der Installation des ersten freigegebenen Druckers wird der Ordner %systemroot%\System32\Spool\Drivers als Print$ freigegeben. Dieser Ordner stellt Zugriff auf die Druckertreiberdateien für Clients bereit. Administratoren und Druck-Operatoren – Vollzugriff, Gruppe Jeder- Lesen (siehe Abbildung 7-8)

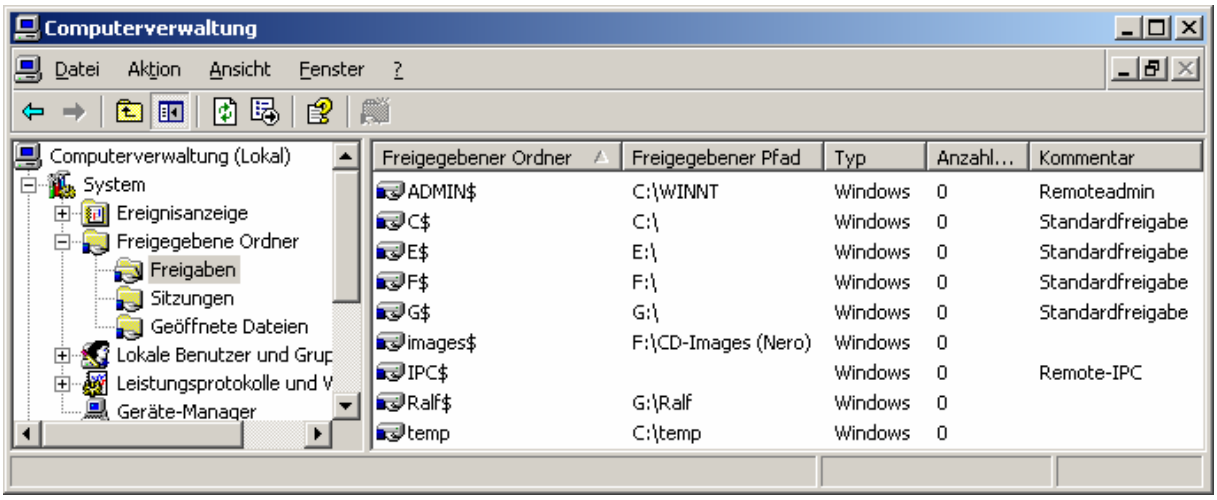


Abbildung 7-8 Anzeige der Freigaben in Computerverwaltung

7.5. Übersicht der Freigaben

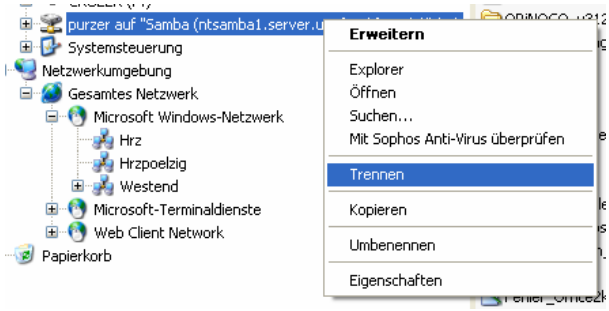


- Ein freigegebener Ordner wird im Windows Explorer durch eine geöffnete Hand gekennzeichnet.
- Eine Übersicht aller auf dem Rechner vorhandenen Freigaben kann über den Befehl „net share“ angezeigt werden, bzw. über „Arbeitsplatz → Verwalten → Freigegebene Ordner → Freigaben“
- Versteckte Ordnerfreigaben sind durch ein „$“-Zeichen am Ende des Freigabenamens gekennzeichnet. Diese Freigaben sind in der Netzwerkumgebung nicht sichtbar und nur über explizites „mounten“ der Freigabe verfügbar.

7.6. Trennen der Netzwerklaufwerke

Wenn Sie die Netzwerklaufwerke nicht mehr benötigen, können Sie diese trennen indem Sie

- im Explorer mit der rechten Maustaste auf den Laufwerksbuchstaben gehen und dort „Trennen“ wählen.
- im Explorer unter „Extras → Netzlaufwerke trennen“ das entsprechende Netzlaufwerk trennen.



Achten Sie beim Trennen der Netzlaufwerke darauf, dass keine Dateien/Fenster der Daten auf dem Netzlaufwerk mehr offen sind. Schließen Sie also alle offenen Dateien/Fenster.

7.7. Anwenden von Berechtigungen für freigegebene Ordner

Effektive Berechtigungen – ein Benutzer kann Mitglied mehrerer Gruppen sein, die mit verschiedenen Berechtigungen für den Zugriff auf einen freigegebenen Ordner ausgestattet sind.
Verweigern von Berechtigungen – Verweigerte Berechtigungen setzen Berechtigungen außer Kraft, die einem Benutzerkonto oder einer Gruppe an anderer Stelle gewährt wurden.

NTFS-Berechtigungen – Berechtigungen für freigegebene Ordner ermöglichen den Zugriff auf die Dateien und Ordner eines FAT-Volumes, reichen jedoch für Zugriff auf die Dateien und Ordner eines NTFS-Volumes nicht aus. Beim Zugriff auf einen freigegebenen Ordner, der sich auf einem NTFS-Volume befindet, muss der Benutzer sowohl über Berechtigungen für den freigegebenen Ordner als auch über entsprechende NTFS-Berechtigungen für den Zugriff auf die Ordnerinhalte verfügen. Die effektiven Berechtigungen sind auf einem NTFS-Volume durch die Freigabeberechtigungen eingeschränkt.

Wenn man einen freigegebenen Ordner kopiert, ist der ursprünglicher Ordner weiterhin freigegeben, der kopierte jedoch nicht. Bei einer Umbenennung oder Verschiebung wird die Freigabe für diesen Ordner aufgehoben.

8. Überwachung

Überwachungsrichtlinien dienen u.a. dazu, Zugriffe auf Objekte (also z.B. Dateien und Ordner) oder auch fremde Einloggversuche auf den Rechner festzustellen.
Die Protokolle werden in der Computerverwaltung → Ereignisanzeige → Sicherheit geführt.
Wenn man die Überwachungsrichtlinien nutzen möchte, muss man diese zuerst in den Gruppenrichtlinien (Start → ausführen → gpedit.msc) einschalten, da sie standardmässig deaktiviert sind (siehe Abbildung 8-1).

Lokale Sicherheitsrichtlinie -> Lokale Richtlinien -> Überwachungsrichtlinien-> Objektzugriffsversuche überwachen aktivieren

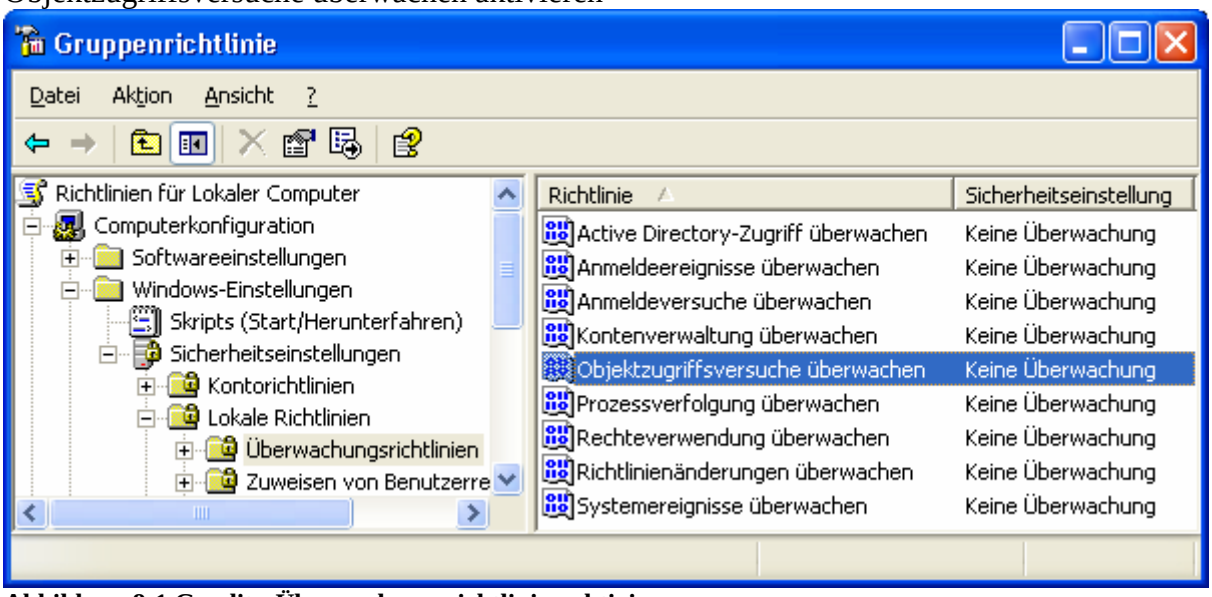


Abbildung 8-1 Gpedit - Überwachungsrichtlinien aktivieren

Sie müssen nun noch festlegen, für welchen Nutzer (bzw. welche Benutzergruppen) welche Objekte (Verzeichniszugriff, Dateizugriff etc.) überwacht werden soll. Dies legen Sie in den Eigenschaften des Objekts (Ordner, Datei) fest (siehe Abbildung 8-2).
Sicherheit → Erweitert → Überwachung -> Benutzer oder Gruppe wählen, Zugriffereignisse die überwacht werden sollen, selektieren → OK drücken

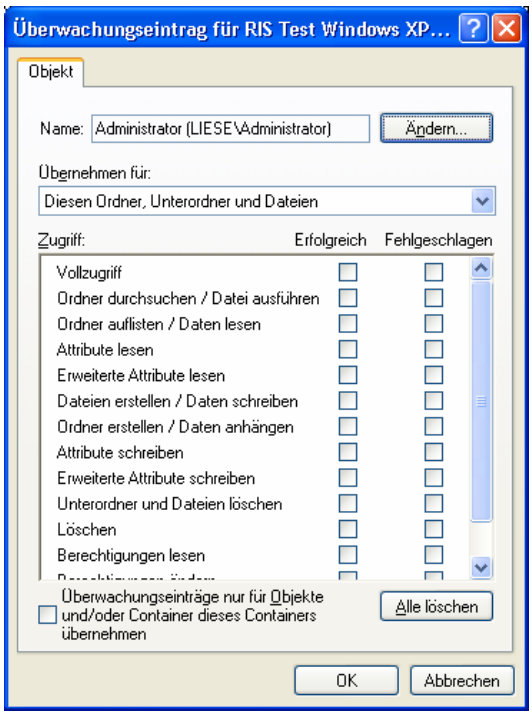


Abbildung 8-2 Überwachungseinstellungen festlegen

Nachdem die Überwachung richtig eingestellt wurde, kann man alle Ereignisse, die den Überwachungskriterien entsprechen, in dem Sicherheitsprotokoll der Ereignisanzeige des Systems sehen. Da die Protokolldateien schnell sehr unübersichtlich und auch groß werden, sollten Sie

- nur die notwendigen Ereignisse überwachen
- bei der Auswertung der Ereignisse in der Ereignisanzeige den Filter benutzen (Ansicht → Filter)
- die Größe der Logdatei in der Ereignisanzeige beschränken und festlegen, was bei Erreichen der maximalen Protokollgröße geschehen soll (siehe Abbildung 8-3).

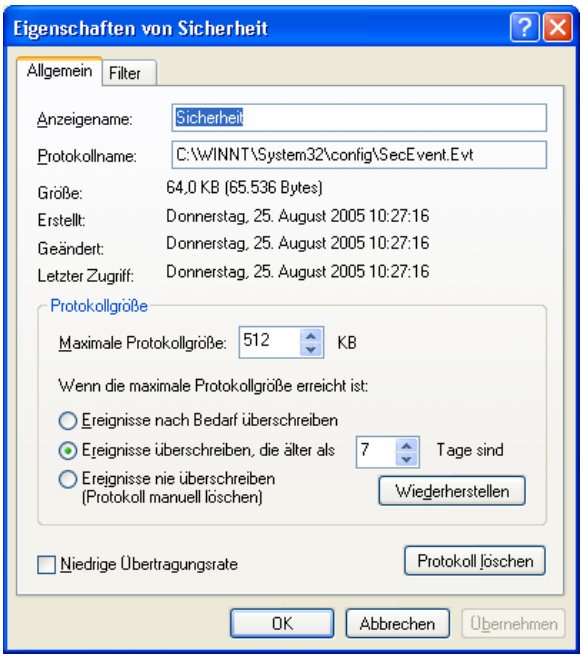


Abbildung 8-3 Eigenschaften Sicherheitsprotokoll

8.1. Zusammenfassung: Richtlinien für die Berechtigungsvergabe bei freigegebenen Ordnern

- Ermitteln Sie, welche Benutzer und Gruppen Zugriff auf eine Ressource benötigen und in welchem Umfang (wer braucht welche Rechte). Dokumentieren Sie die Berechtigungsvergabe für jede Ressource.

- Weisen Sie NTFS- sowie Freigabeberechtigungen nicht auf Benutzer- sondern auf Gruppenebene zu, um die Zugriffsverwaltung zu vereinfachen.

- Vergeben Sie möglichst einschränkende Berechtigungen. Erlauben Sie nur das, was notwendig ist.

- Fassen Sie Ordner mit gleichen Sicherheitsanforderungen in einem Ordner zusammen. Legen Sie auf dem obersten Ordner die Rechte fest und arbeiten Sie mit der NTFS Berechtigungsvererbung.

- Verwenden Sie aussagekräftige Freigabenamen (max. 80 Zeichen) mit „Standardisierten Namen“ um die Übersicht zu behalten (z.B. FB00_Botanik_HIWIS$)

8.2. Offlinezugriff auf Dateien im Netz

Berechtigungen: Legt die Rechte beim Zugriff über das Netz für Benutzer (oder Benutzergruppen) fest:

- Lesen
- Ändern
- Vollzugriff

Zwischenspeichern (die Einstellungen, mit denen der Offlinezugriff auf diesen freigegeben Ordner konfiguriert wird). Ist voreingestellt, muss aber auf Client-Seite noch konfiguriert werden (Windows Explorer → Extras → Ordneroptionen → Offlinedateien → Aktivieren) sofern es benutzt werden soll.

- Bei XP **muss die schnelle Benutzerumschaltung deaktiviert werden**, um dieses Feature nutzen zu können.
- Im Explorer müssen „Offlinedateien“ aktiviert sein (Extras → Ordneroptionen → Offlinedateien).
- Es werden nicht alle Dateien standardmäßig offline zur Verfügung gestellt (siehe auch http://support.microsoft.com/kb/252509/EN-US/) .

- **Manuelles Zwischenspeichern** von Dokumenten (Standardeinstellung). Man muss vorher manuell angeben (rechter Mausklick drauf), welche Dateien/Ordner Offline zur Verfügung stehen sollen.
- **Automatisches Zwischenspeichern** von Dokumenten – jede Datei, die im freigegebenen Ordner geöffnet wird, wird für den Benutzer offline verfügbar gemacht. Nicht geöffnete Dateien stehen offline nicht zur Verfügung. Bei jedem Öffnen einer Datei wird die ältere Kopie der Datei automatisch gelöscht.

- **Automatisches Zwischenspeichern** von Programmen und Dokumenten – bietet Offlinezugriff auf freigegebene Ordner mit Dateien, die gelesen oder ausgeführt, dabei aber nicht geändert werden. Mit der Einstellung wird der Datenverkehr im Netzwerk reduziert (siehe Abbildung 8-4)



Abbildung 8-4 Offline verfügbar machen