Berechtigungen

Autor: Schmid Tobias

Datum: 19.10.2015

Typ: Information

Version: 1.0

Inhaltsverzeichnis

INHALT

1 Was sind Berechtigungen?

Jedem Container bzw. Objekt in einem Netzwerk sind bestimmte Informationen für die Zugriffssteuerung zugewiesen. Diese werden als Sicherheitsbeschreibung bezeichnet und steuern den Benutzern und Gruppen gewährten Zugriff auf das entsprechende Objekt. Die Sicherheitsbeschreibung wird automatisch in Verbindung mit dem Container oder Objekt erstellt. Ein typisches Beispiel für ein Objekt mit einer Sicherheitsbeschreibung ist eine Datei.

Berechtigungen werden in der Sicherheitsbeschreibung eines Objekts festgelegt. Die Berechtigungen werden bestimmten Benutzern bzw. Gruppen zugewiesen oder beziehen sich auf diese. Für die Datei **Temp.dat** kann die integrierte Gruppe **Administratoren** z. B. über die Berechtigungen **Lesen**, **Schreiben** und **Löschen**, die Gruppe **Operatoren** hingegen nur über die Berechtigungen **Lesen** und **Schreiben** verfügen.

Jede Zuweisung von Berechtigungen für einen Benutzer oder eine Gruppe wird im System als Zugriffssteuerungseintrag (Access Control Entry, ACE) dargestellt. Die Gesamtheit der Berechtigungseinträge in einer Sicherheitsbeschreibung wird als Berechtigungssatz oder Zugriffssteuerungsliste (Access Control List, ACL) bezeichnet. Daher enthält der Berechtigungssatz für die Datei **Temp.dat** zwei Berechtigungseinträge, einen für die integrierte Gruppe **Administratoren** und einen für die Gruppe **Sicherungs-Operatoren**.

1.1 Explizite und vererbte Berechtigungen

Es gibt zwei Arten von Berechtigungen: explizite und vererbte Berechtigungen.

Explizite Berechtigungen sind Berechtigungen, die standardmäßig für nicht untergeordnete Objekte festgelegt werden, wenn das Objekt erstellt wird, oder durch Benutzeraktionen für nicht untergeordnete, übergeordnete oder untergeordnete Objekte.

Vererbte Berechtigungen werden von einem übergeordneten Objekt auf ein Objekt übertragen. Dies erleichtert die Verwaltung von Berechtigungen und stellt die einheitliche Zuweisung von Berechtigungen zu sämtlichen Objekten innerhalb eines Containers sicher.

In der Standardeinstellung werden beim Erstellen von Objekten die Berechtigungen des übergeordneten Containers automatisch auf diese Objekte übertragen. Wenn Sie z. B. den Ordner **EigenerOrdner** erstellen, werden die für den Ordner festgelegten Berechtigungen automatisch an sämtliche in diesem Ordner erstellten Unterordner und Dateien vererbt. Dem Ordner **EigenerOrdner** sind also explizite Berechtigungen angefügt, während die Unterordner und Dateien innerhalb dieses Ordners über vererbte Berechtigungen verfügen.

Hinweis

Geerbte Zugriffsverweigerungen verhindern nicht den Zugriff auf ein Objekt, wenn das Objekt über eine explizite Zugriffsgenehmigung verfügt. Explizite Berechtigungen haben Vorrang vor geerbten Berechtigungen, auch vor geerbten Zugriffsverweigerungen.

2 Berechtigung 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					
Synchronisieren	x	x	x	x	x	x

Wichtig

Gruppen oder Benutzer, denen für einen Ordner die Berechtigung Vollzugriff erteilt wurde, können alle Dateien in diesem Ordner löschen – unabhängig von den Berechtigungen, durch die die Dateien geschützt werden.

2.1 Weitere Überlegungen

Die Optionen Ordnerinhalt auflisten und Lesen und Ausführen weisen scheinbar dieselben speziellen Berechtigungen auf. Diese Berechtigungen werden jedoch auf unterschiedliche Weise übernommen. Die Berechtigungen für Ordnerinhalt auflisten werden nur von Ordnern übernommen, nicht jedoch von Dateien. Diese Option sollte nur dann auftreten, wenn Sie Berechtigungen für Ordner anzeigen. Bei Lesen und Ausführen dagegen werden die Berechtigungen sowohl von den Dateien als auch von den Ordnern übernommen. Diese Option ist immer verfügbar, wenn Sie Berechtigungen für Dateien oder Ordner anzeigen.

In dieser Version von Windows enthält die Gruppe **Jeder** nicht standardmäßig die Gruppe Anonyme Anmeldung. Demnach wirken sich auf die Gruppe **Jeder** angewendete Berechtigungen nicht auf die Gruppe **Anonyme Anmeldung** aus.

3 Freigabe und NTFS Berechtigungen auf einem Dateiserver

Der Zugriff auf einen Ordner auf einem Dateiserver kann über zwei Berechtigungseintragssätze bestimmt werden: den Freigabeberechtigungssatz für einen Ordner und den NTFS-Berechtigungssatz für den Ordner (der auch für Dateien festgelegt werden kann). Freigabeberechtigungen werden oft verwendet für das Verwalten von Computern mit FAT32-Dateisystemen oder von anderen Computern, die das NTFS-Dateisystem nicht verwenden.

Freigabeberechtigungen und NTFS-Berechtigungen sind insofern unabhängig voneinander, als dass sie sich nicht gegenseitig ändern. Zum Bestimmen der endgültigen Zugriffsberechtigungen für einen freigegebenen Ordner wird sowohl der Freigabeberechtigungseintrag als auch der NTFS-Berechtigungseintrag berücksichtigt. Es werden dann die Berechtigungen mit den größten Einschränkungen angewendet.

In der folgenden Tabelle werden äquivalente Berechtigungen vorgeschlagen, die der Gruppe **Benutzer** für bestimmte freigegebene Ordnertypen durch einen Administrator erteilt werden können. Eine weitere Herangehensweise besteht darin, Freigabeberechtigungen für die Gruppe **Jeder** auf **Vollzugriff** festzulegen und ausschließlich auf NTFS-Berechtigungen zurückzugreifen, um den Zugriff einzuschränken.

Ordnertyp	Freigabeberechtigungen	NTFS-Berechtigungen
Öffentlicher Ordner: Ein Ordner, auf den jeder zugreifen kann.	Erteilen Sie der Gruppe **Benutzer** die Berechtigung **Ändern**.	Erteilen Sie der Gruppe **Benutzer** die Berechtigung **Ändern**.
Ablageordner: Ein Ordner, in dem Benutzer vertrauliche Berichte oder Hausaufgaben ablegen können, die nur der Abteilungsleiter oder Kursleiter lesen kann.	Erteilen Sie der Gruppe **Benutzer** die Berechtigung **Ändern**. Erteilen Sie der Gruppenleitung die Berechtigung **Vollzugriff**.	Erteilen Sie der Gruppe **Benutzer** eine Schreibberechtigung, die auf **Nur diesen Ordner** angewendet wird. (Diese Option ist auf der Seite **Erweitert** verfügbar.) Wenn jeder Benutzer bestimmte Berechtigungen für die von ihm abgelegten Dateien benötigt, können Sie einen Berechtigungseintrag für den bekannten Sicherheitsbezeichner (Security Identifier, SID) des Ersteller-Besitzers erstellen und diesen auf **Nur Unterordner und Dateien** anwenden. Beispielsweise können Sie dem SID des Ersteller-Besitzers Lese- und Schreibberechtigung für den Ablageordner erteilen und diese auf alle Unterordner und Dateien anwenden. Dadurch wird dem Benutzer, der die Datei abgelegt oder erstellt hat (der Ersteller-Besitzer), die Möglichkeit gegeben, die Datei zu lesen und in sie zu schreiben. Der Ersteller-Besitzer kann dann über den Befehl **Ausführen** mithilfe von *\\ServerName\DropFolder\FileName* auf die Datei zugreifen. Erteilen Sie der Gruppenleitung die Berechtigung **Vollzugriff**.
Anwendungsordner: Ein Ordner mit Anwendungen, die über das Netzwerk ausgeführt werden können.	Erteilen Sie der Gruppe **Benutzer** eine Leseberechtigung.	Erteilen Sie der Gruppe **Benutzer** die Berechtigungen **Lesen**, **Lesen und Ausführen** und **Ordnerinhalt auflisten**.
Basisordner: Ein einzelner Ordner für jeden Benutzer. Nur der Benutzer hat Zugriff auf den Ordner.	Erteilen Sie den einzelnen Benutzern für den entsprechenden Ordner die Berechtigung **Vollzugriff**.	Erteilen Sie den einzelnen Benutzern für den entsprechenden Ordner die Berechtigung **Vollzugriff**.

3.1 Weitere Überlegungen

Wenn Sie einem Benutzer die NTFS-Berechtigung **Vollzugriff** für einen Ordner erteilen, kann dieser Benutzer den Besitz des Ordners übernehmen, solange der Benutzer nicht anderweitig eingeschränkt ist. Gehen Sie mit dem Erteilen des Vollzugriffs vorsichtig um.

Wenn Sie für die Verwaltung des Zugriffs auf Ordner ausschließlich NTFS-Berechtigungen verwenden möchten, legen Sie für die Freigabeberechtigungen den Vollzugriff für die Gruppe **Jeder** fest.

NTFS-Berechtigungen wirken sich sowohl auf den lokalen als auch auf den Remotezugriff aus. NTFS-Berechtigungen gelten unabhängig vom Protokoll. Freigabeberechtigungen hingegen gelten nur für Netzwerkfreigaben. Mit Freigabeberechtigungen wird der Zugriff für den Computer, für den Sie Freigabeberechtigungen festgelegt haben, nicht auf einen lokalen Benutzer oder auf einen Terminalserverbenutzer eingeschränkt. Demnach wird mit Freigabeberechtigungen kein Datenschutz zwischen Benutzern an einem Computer bereitgestellt, der von mehreren Benutzern verwendet wird. Dies gilt ebenso für einen Terminalserver, auf den mehrere Benutzer zugreifen.

Standardmäßig beinhaltet die Gruppe **Jeder** nicht die Gruppe **Anonym**, sodass auf die Gruppe **Jeder** angewendete Berechtigungen sich nicht auf die Gruppe **Anonym** auswirken.

4 Vererbte Berechtigungen

Vererbte Berechtigungen werden von einem übergeordneten Objekt auf ein Objekt übertragen. Dies erleichtert die Verwaltung von Berechtigungen und stellt die einheitliche Zuweisung von Berechtigungen zu sämtlichen Objekten innerhalb eines Containers sicher.

4.1 Vererbung für alle Objekte

Wenn die Kontrollkästchen für Berechtigungen unter **Zulassen** und **Verweigern** in den verschiedenen Teilen der Benutzeroberfläche für die Zugriffssteuerung schattiert sind, während Sie die Berechtigungen eines Objekts anzeigen, hat das Objekt die Berechtigungen von einem übergeordneten Objekt geerbt. Sie können diese geerbten Berechtigungen auf der Registerkarte **Berechtigungen** der Eigenschaftenseite **Erweiterte Sicherheitseinstellungen** festlegen.
Änderungen an den geerbten Berechtigungen können auf drei verschiedene empfohlene Arten vorgenommen werden:
Nehmen Sie Änderungen am übergeordneten Objekt vor, wo die Berechtigungen explizit definiert sind. Das untergeordnete Objekt erbt daraufhin diese Berechtigungen. Weitere Informationen finden Sie unter Festlegen, Anzeigen, Ändern oder Entfernen von Berechtigungen für ein Objekt.
Wählen Sie die Berechtigung **Zulassen** aus, um die vererbte Berechtigung **Verweigern** zu überschreiben.
Deaktivieren Sie das Kontrollkästchen **Vererbbare Berechtigungen des übergeordneten Objektes einschließen**. Anschließend können Sie Änderungen an den Berechtigungen vornehmen oder Benutzer und Gruppen aus der Liste **Berechtigungen** entfernen. Das Objekt erbt nun jedoch keine weiteren Berechtigungen des übergeordneten Objekts.

Hinweis

Geerbte Zugriffsverweigerungen verhindern nicht den Zugriff auf ein Objekt, wenn das Objekt über eine explizite Zugriffsgenehmigung verfügt.

Hinweis

Explizite Berechtigungen haben Vorrang vor geerbten Berechtigungen, auch vor geerbten Zugriffsverweigerungen.

Wenn unter **Berechtigungen für <Benutzer oder Gruppe>** der Eintrag **Spezielle Berechtigungen** ausgeblendet angezeigt wird, bedeutet dies nicht, dass diese Berechtigung vererbt wurde. Es bedeutet vielmehr, dass eine spezielle Berechtigung ausgewählt wurde.

Auf der Registerkarte **Berechtigungen** der Seite **Erweiterte Sicherheitseinstellungen für <Ordner>** werden in der Spalte **Übernehmen für** unter **Berechtigungseinträge** die Ordner oder Unterordner angezeigt, auf die eine Berechtigung angewendet wird. In der Spalte **Geerbt von** wird angezeigt, von welchem Objekt die Berechtigungen geerbt wurden.

Mithilfe des Felds **Anwenden auf** der Seite **Berechtigungseintrag für<Ordner>** können Sie die Ordner oder Unterordner auswählen, auf die die Berechtigungen angewendet werden sollen.

5 Freigabe- und NTFS-Berechtigungen unter Windows

Das Verwalten von Benutzerrechten und Freigaben von Verzeichnissen und Dateien, gehört für einen Administrator zur täglichen Arbeit. Leider stolpert man allzu oft über Windows Freigaben, die unterschiedlichen Gruppen Vollzugriff gewährt. Dies stellt grundsätzlich kein Problem dar und wenn man damit richtig umgeht, ist ein sicheres Arbeiten möglich. Die richtige Kombination mit Freigaben und NTFS-Rechten ist hier der Schlüssel zum Erfolg. Leider schleichen sich genau in dieser Kombination sehr oft Fehler ein. Zum Schutz aller Administratoren muss ich hier erwähnen, dass dies meisten unbewusst und aus historischen Gründen geschieht.

Mögliche Grundregeln lauten:

Vollzugriff auf NTFS-Ebene bekommen nur die, die Wissen was sie tun (oder die es wissen sollten) – also nur die Administratoren

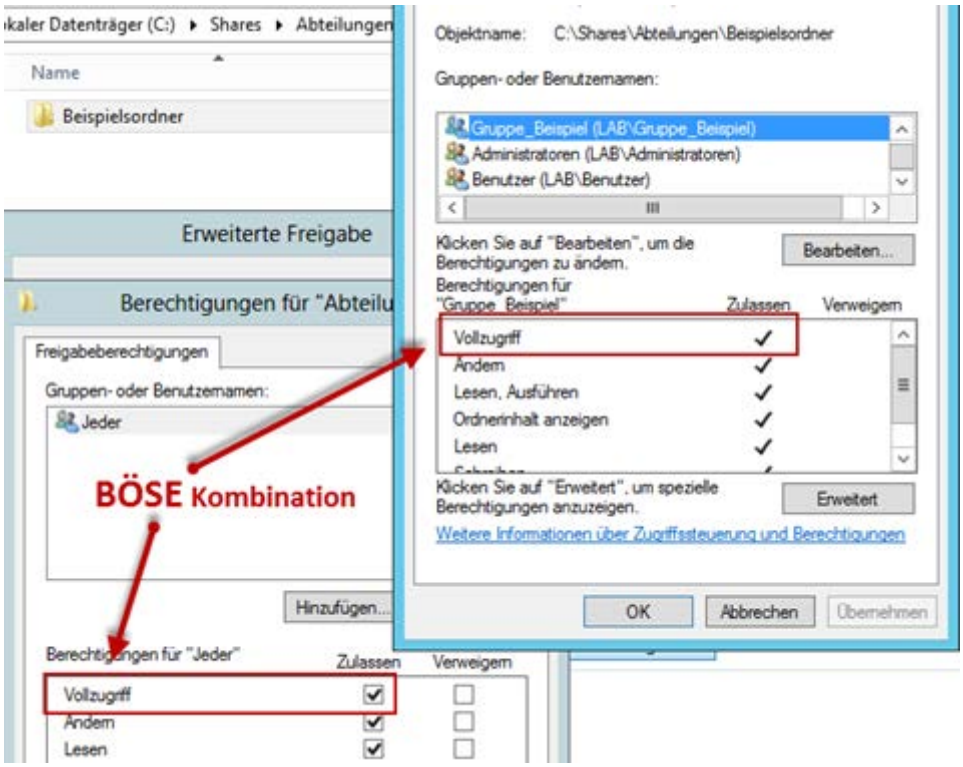
Rechte nur auf Gruppen nie Einzelpersonen

Nur Rechte gewähren die notwendig sind

Kein "Verweigern"

6 Wie man es nicht machen sollte

Nachfolgendes sieht man oft in der Praxis:



Vollzugriff auf Freigabe- und NTFS-Rechte ist eine Böse Kombination

6.1 Warum?

Weil ich als verantwortliche Person keine Kontrolle über die Zugriffsrechte habe. Vollzugriff impliziert das Recht, dass ich Berechtigungen ändern, den Besitz übernehmen und nicht eigene Unterordner und Dateien löschen darf.

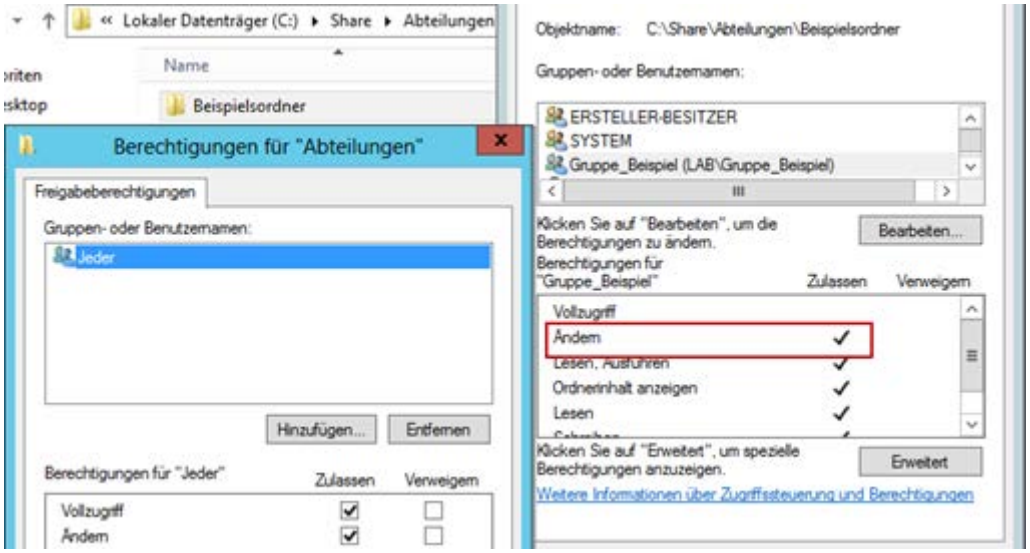
Also alles was man nicht erlauben möchte und somit kurzum eine schlechte Idee.

6.2 Und wie mache ich es richtig?

Viele Wege führen nach Rom, so auch in diesem Fall. Ich verwende zumeist zwei Varianten, die ich hier kurz vorstellen möchte.

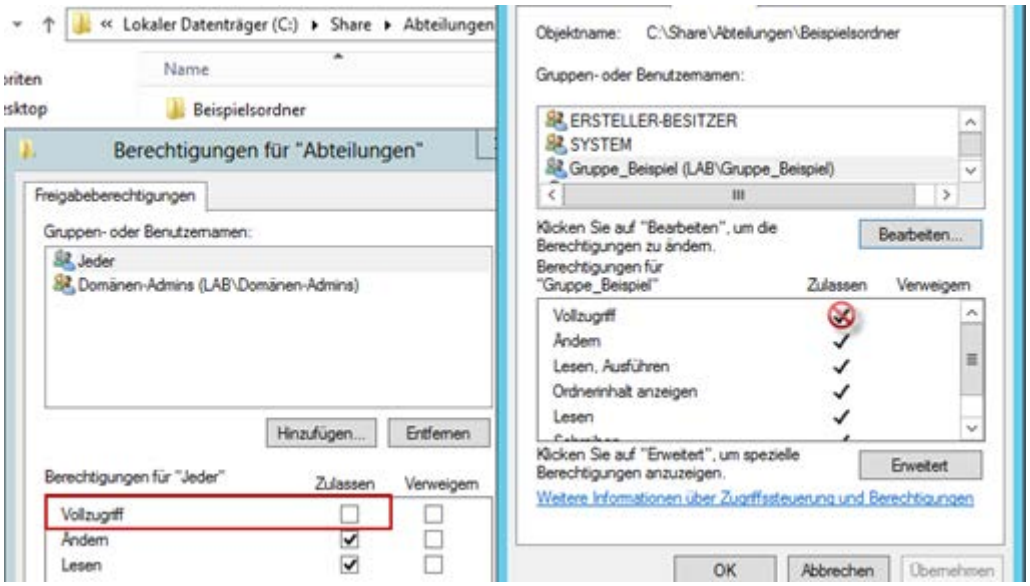
6.2.1 Reine NTFS-Berechtigungen

Hierbei bleibt auf der Freigabeberechtigung die Gruppe “Jeder” mit Vollzugriff bestehen und die “**Gruppe_Beispiel”**erhält nur das Recht “Ändern”.



6.2.2 Kombination aus Freigabe- und NTFS-Berechtigung

Auf der Freigabeberechtigung erhält die Gruppe “Jeder” das Recht “Ändern”, die “**Domänen-Admins**” Vollzugriff. Somit hat die NTFS-Berechtigung der **“Gruppe_Beispiel”** keine Auswirkungen. Zur Klarheit sollte man aber trotzdem die Rechte auf “Ändern” setzen.



Diese Variante verzeiht Fehler in der NTFS-Berechtigungen, die erste nicht.

7 Freigabeberechtigung

Die Freigabeberechtigung ist die zentrale Verwaltung in der Domäne um Ressourcen zur Verfügung zu stellen und stammt noch aus der Zeit von OS/2. Dahinter verbirgt sich der LAN Manager, der es den Clients ermöglicht die Ressourcen zu verwenden.

Die Rechte beschränken sich im auf drei Arten:

Vollzugriff
Dateien und Ordner können innerhalb der Freigabe gelesen, verändert, angelegt, gestartet und Berechtigungen verändert werden, sofern die NTFS-Rechte nicht entgegenstehen.
Ändern
Dateien und Ordner können innerhalb der Freigabe gelesen, verändert, angelegt und gestartet werden, sofern die NTFS-Rechte nicht entgegenstehen.
Lesen
Dateien und Ordner können innerhalb der Freigabe gelesen und gestartet werden, sofern die NTFS-Rechte nicht entgegenstehen.

Hinweise:

Freigabeberechtigungen gelten nur für den Remotezugriff. Lokale Berechtigungen werden nicht tangiert.
Wenn man ausschließlich über NTFS-Berechtigungen die Zugriffe steuern möchte, so ist auf der Freigabe “Jeder” mit Vollzugriff zu versehen.

8 NTFS-Berechtigung

Die NTFS-Berechtigungen wurden immer weiter entwickelt und beinhalten zum heutigen Stand (Windows Server 2012) nachfolgende Rechte:

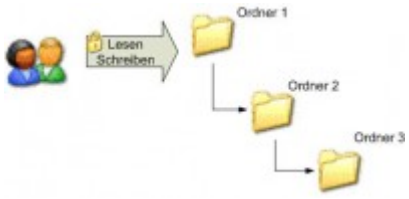
Spezielle Berechtigungen	Vollzugriff	Ändern	Lesen, Ausführen	Oderinhalt anzeigen	Lesen	Schreiben
Vollzugriff	**X**					
Ordner durchsuchen /Datei ausführen	**X**	**X**	**X**	**X**		
Ordern auflisten / Daten lesen	**X**	**X**	**X**	**X**	**X**	
Attribute lesen	**X**	**X**	**X**	**X**	**X**	
Erweiterte 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**					

“Lesen, Ausführen” und “**Ordnerinhalt anzeigen”** geben anscheinend die gleichen Berechtigungen wieder. Es wird jedoch auf unterschiedliche Art interpretiert. “**Ordnerinhalt anzeigen”** werden nur von Ordner übernommen, nicht von Dateien. “**Lesen, Ausführen”** wird sowohl für Ordner, als auch für Dateien übernommen.
Gruppen und Benutzern, denen Vollzugriff auf einen Ordner erteilt wurde, können alle Dateien in diesem Ordner löschen, dabei spielt es keine Rolle, ob die Dateien durch andere Berechtigungen geschützt werden.
Die NTFS-Berechtigungen regeln den lokalen- und den Remotezugriff.

9 NTFS-Berechtigungen

9.1 Vererbung Von NTFS-Berechtigungen

Die Vererbung der Berechtigungen vereinfacht das Handling mit Ordnern, untergeordneten Ordnern und Ressourcen, um den Zugriff auf diese zu gewähren. Standardmäßig werden Berechtigungen vom übergeordnetem Ordner auf die darunterliegenden Ordner vererbt, diese besitzen dann die gleichen Berechtigungen.



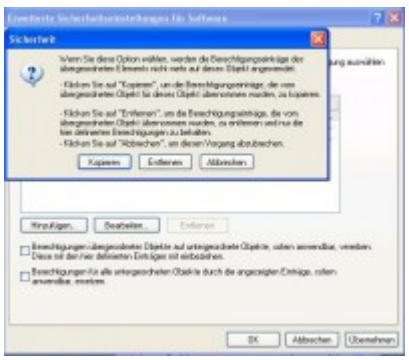
Manchmal ist es aber sinnvoll, diese Vererbung zu unterbrechen, um den darunterliegenden Unterordnern explizit neue Berechtigungen zugeben. Beispiel: alle Mitglieder einer Gruppe haben Zugriff auf Ordner 1 und der Abteilungsleiter soll alleinigen Zugriff auf Ordner 2 und 3 haben.

9.2 Steuern der Vererbung

Wenn die Vererbung blockiert wird gibt es 2 Möglichkeiten:

Kopieren -- geerbte Berechtigungen werden aus dem übergeordnetem Ordner kopiert

Entfernen -- geerbte Berechtigungen aus dem übergeordneten Ordner werden entfernt und durch explizit zugewiesene ersetzt



9.3 Besonderheiten beim Kopieren und Verschieben

Beim kopieren und Verschieben von Ordner und Dateien mit NTFS-Berechtigungen müssen noch einige Besonderheiten beachtet werden.

9.3.1 Kopieren

Kopieren innerhalb einer NTFS-Partition -- erbt die Kopie die Berechtigungen des Zielordners

Kopieren in eine andere NTFS-Partition -- erbt die Kopie die Berechtigungen des Zielordners

Kopieren in eine nicht NTFS-Partition z.B. FAT-Partition --verliert die Kopie die Berechtigungen, weil FAT keine NTFS-Berechtigungen kennt

9.3.2 Verschieben

Verschieben innerhalb einer NTFS-Partition -- behält die ursprünglichen Berechtigungen, werden die Berechtigungen des übergeordneten Ordners später geändert werden die Änderungen übernommen, explizite Berechtigungen bleiben erhalten

Verschieben in eine andere NTFS-Partition -- erbt die Berechtigungen des Zielordners

Verschieben in eine nicht NTFS-Partition z.B. FAT-Partition --verliert die Berechtigungen, weil FAT keine NTFS-Berechtigungen kennt

10 Weiterführende Links

Microsoft

https://technet.microsoft.com/de-ch/library/cc754178.aspx

https://technet.microsoft.com/de-de/library/cc770962.aspx