Best Practice für Berechtigungsvergabe auf Fileservern

aikux.com GmbH

Oldenburger Straße 37

10551 Berlin

Tel +49 30 8095010-40

Fax +49 30 8095010-41

E-Mail: info@aikux.com

WWW: http://www.aikux.com

Autor: Dirk Menzer

Revision 1.1 vom 15.08.2012

aikux.com

Inhalt

1. Einleitung

Dieses Dokument soll als Einführung in die Berechtigungsvergabe auf Fileservern dienen. Es wird erläutert, welche Berechtigungen es gibt, wie man sie vergibt und welche Überlegungen dazu von Nöten sind.
Berechtigungen regeln den Zugriff auf die Dateien, weshalb es wichtig ist, ihre Vergabe wohldurchdacht zu handhaben. Sind die Berechtigungen zu locker vergeben, kann unter Umständen jeder auf die Arbeitsverträge aller Mitarbeiter oder andere geheime Daten zugreifen. Sind sie jedoch zu restriktiv vergeben, wird das Arbeiten erschwert, da eventuell Mitarbeiter nicht auf für sie relevante Daten zugreifen können, um sie zu bearbeiten.
Weiterhin ist es auch sinnvoll, die Rechtevergabe so transparent wie möglich zu gestalten, da es sonst fast unmöglich wird, die Rechte zu administrieren, wenn in den NTFS-Rechten keine Übersicht mehr gegeben ist. Darüber hinaus sollten auch spezielle Gruppen für die Berechtigungen genutzt werden, die man möglichst nicht für andere Zwecke „missbrauchen“ sollte.

2. Berechtigungen

Berechtigungen sind auf jedem Fileserver notwendig, damit nur die Benutzer auf Dokumente zugreifen können, die es auch sollen. Es gibt verschiedene Varianten, das zu ermöglichen. Zum ersten sind es die Share-Berechtigungen, die man allerdings so offen wie möglich gestalten sollte (z.B. authentifizierte Benutzer → Vollzugriff), um letztendlich den Zugriff über die NTFS-Berechtigungen (Berechtigungen im Filesystem) einzuschränken. Bei der Vergabe von Berechtigungen ist auch darauf zu achten, dass man diese möglichst flach hält (maximal bis zur 5. Verzeichnisebene ab Share), damit das System noch überschaubar bleibt und das Kerberos-Token (Anmeldetoken, weiter unten genauer erklärt) nicht zu groß wird. Auch sollte darauf geachtet werden, so wenig unterschiedliche Berechtigungen wie möglich zu setze. Das heist, dass man Verzeichnisse anlegt, auf welche die gesamte Abteilung „lesen und ausführen“ bekommt und nur diejenigen User „ändern“ bekommen, die es tatsächlich auch benötigen.

2.1. Zu beachten!

Bei einer Neuinstallation eines Fileservers ist es empfehlenswert, als erstes den „Ersteller und Besitzer“ zu entfernen oder zumindest anzupassen, da dieser „Dummy-User“ bewirkt, dass derjenige, der ein Dokument erstellt, auch der Besitzer wird und Vollzugriffsrechte auf diese Dateien/Ordner erhält. In diesem Fall könnte der Ersteller auch Berechtigungen vergeben oder verweigern mit dem Ergebnis, dass Administratoren oder der Backup-User nicht mehr auf Dateien oder ganze Verzeichnisse zugreifen können.

Wie oben schon erwähnt, sollte man auch die Shares berechtigen. Hier empfiehlt es sich nicht, wie standardmäßig „Jeder“ zu berechtigen, da dazu auch Gäste zählen, sondern das Ganze auf „Authentifizierte Benutzer“ oder noch besser „Domänen-Benutzer“ oder Abteilungsgruppen einzuschränken.

Auch sollte man erwägen, die Shares so anzulegen, dass möglichst keine Shares innerhalb eines anderen Shares entstehen. Eine Verschachtelung der Shares hätte zur Folge, dass man eventuell in einer tieferen Ebene plötzlich Zugriffsrechte bekommt, die aber weiter oben in dem Share nicht ersichtlich sind → Transparenz. Die Shares wählt man deshalb so, dass man schon dadurch einen Zugriff verhindern kann → Denn wenn ein Share nur für eine Abteilung beziehungsweise deren AD-Gruppe zugänglich ist, können andere User gar nicht erst darauf zugreifen.

2.1.1. Das Kerberos-Token-Problem

Das Kerberos-Token dient zur Authentifizierung an Windows-Servern und beinhaltet neben der SID auch die Gruppenzugehörigkeiten. Es ist in der Größe beschränkt und wurde im Laufe der Jahre und über verschiedene Windows-Versionen in seiner Größe angepasst. Wenn ein User allerdings in zu vielen Gruppen Mitglied ist und die maximale Größe des Tokens überschritten wird, können sich die Benutzer nicht mehr an ihrem System anmelden. Darauf ist auch bei der Vergabe der Berechtigungen und Gruppen zu achten.

Lokale Gruppen belegen mehr Speicher als globale oder universelle (der eigenen Domäne), die beiden letztgenannten werden bei der MS Formel mit einem Fünftel der Größe der lokalen Gruppen berechnet. Globale und universelle belegen denselben Speicher. Der

Unterschied ist, dass globale Gruppen nur Benutzerkonten oder andere globale Gruppen aufnehmen können, die zur eigenen Domäne gehören. In universale Gruppen können dagegen Benutzerkonten oder globale Gruppen aller Domänen aufgenommen werden, zu denen eine Vertrauensstellung besteht. Wenn es sich um universelle Gruppen einer anderen Domäne handelt, belegen diese so viel Speicher wie Domänenlokale Gruppen.

2.2. ABE (Access Based Enumeration)

Als weiterer Punkt ist die ABE zu erwähnen. Access-based Enumeration, abgekürzt ABE, bedeutet übersetzt „zugriffsbasierte Auflistung“ oder besser „berechtigungsgesteuerte Auflistung“. Dem Anwender werden im Windows-Explorer nur noch diejenigen Verzeichnisse und Dateien aufgelistet, für die er auch Zugriffsrechte besitzt. Alle anderen Ordner und Dateien sind ausgeblendet.

Die ABE kann man auf Windows 2008 Servern aktivieren, indem man im Servermanager unter „Freigabe- und Speicherverwaltung“ die entsprechende Freigabe auswählt, dort mit einem Rechtsklick die Eigenschaften aufruft, im ersten Reiter (Freigabe) auf „Erweitert“ klickt und dort dann „Zugriffsbasierte Aufzählung aktivieren“ auswählt.

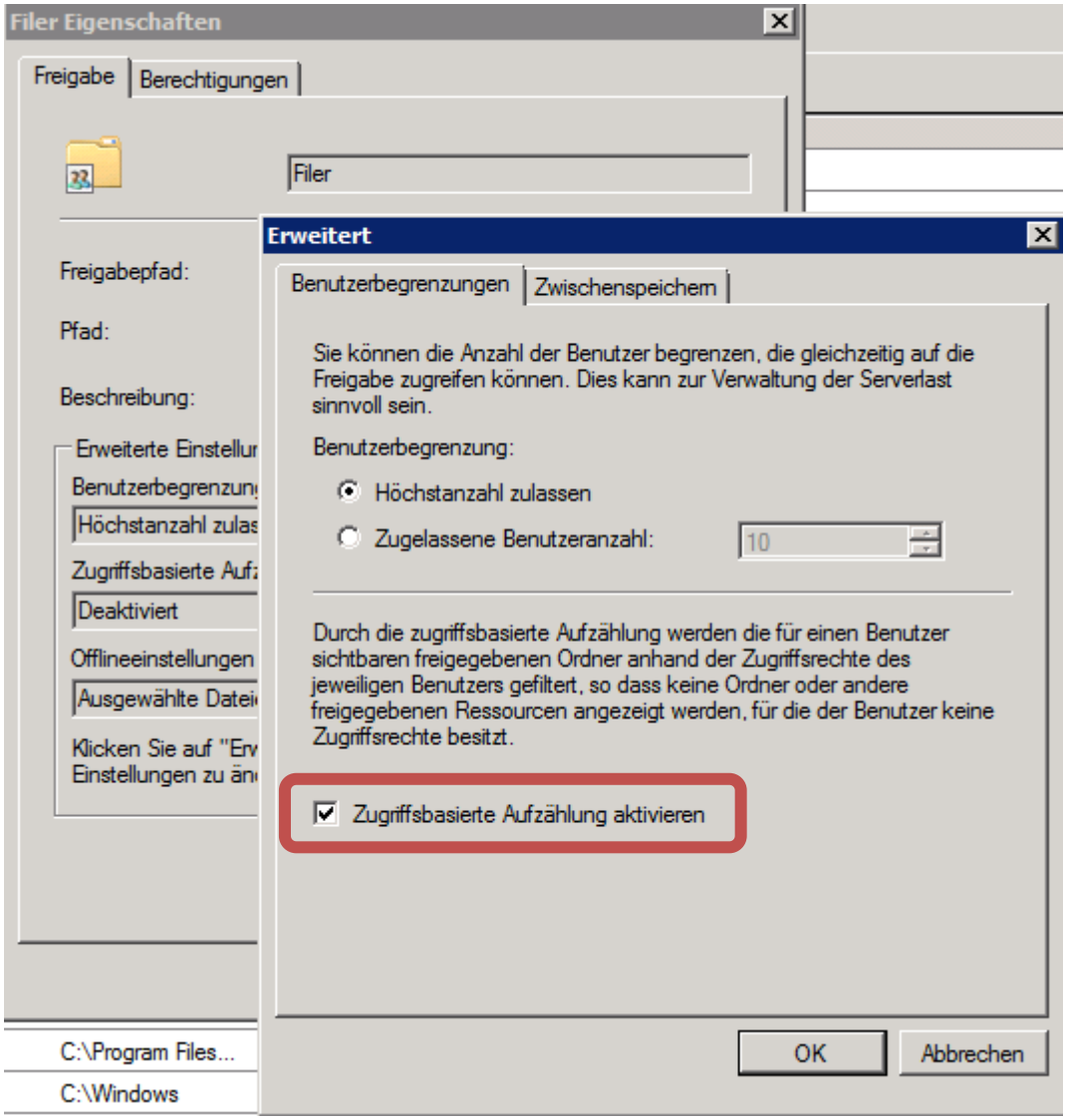

Abbildung 1: Aktivieren der ABE

2.3. NTFS-Berechtigungen

Die NTFS-Berechtigungen sind die Berechtigungen, die im Filesystem ansetzen und dort den Zugriff der User regeln. Es gibt verschiedene NTFS-Berechtigungen, um Zugriffe zu erlauben oder diese zu verweigern.

Folgende Berechtigungen stehen zur Auswahl:

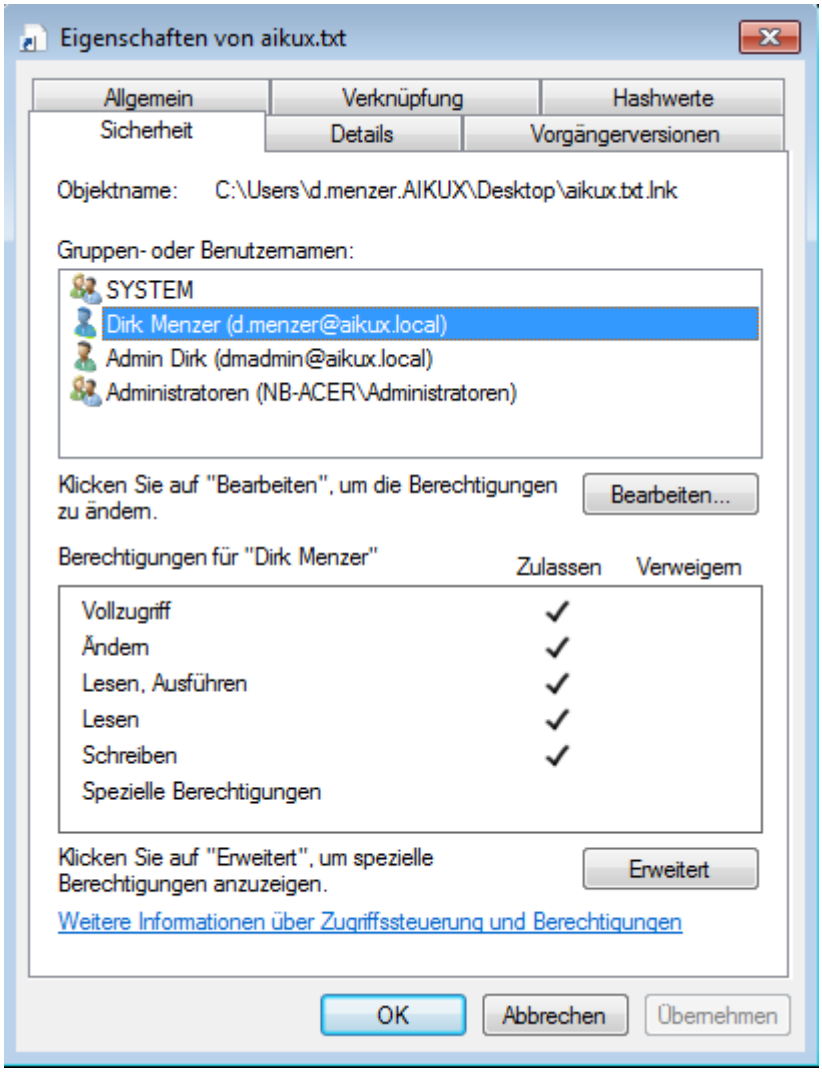

Abbildung 2: Zur Verfügung stehende Standardrechte

- **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 alle Aktionen, welche die Berechtigung „Lesen“ gestattet.
- **Ändern** – Ändern und Löschen von Dateien, Ausführen von Aktionen, welche die Berechtigungen „Schreiben“, „Lesen und Ausführen“ gestatten.
- **Vollzugriff** - Ändern von Berechtigungen, Besitzübernahme, Ausführen von Aktionen, die alle übrigen NTFS-Ordnerberechtigungen gestatten.

Es wird oft angenommen, dass man zum Erstellen, Öffnen, Bearbeiten und Löschen von Ordnern und Dateien auch die Berechtigung „Vollzugriff“ benötigt. Das ist falsch. Es wird lediglich das Recht „Ändern“ benötigt. „Ändern“ beinhaltet all das, was ein normaler User zum Arbeiten braucht. Das Recht „Vollzugriff“ gibt dem User das Recht, auch

Berechtigungen zu ändern bzw. zu vergeben, was in einer Firma den Administratoren vorbehalten bleiben sollte, um ein Chaos in der Berechtigungsvergabe zu vermeiden. Zur Erläuterung: Durch ein Vollzugriffsrecht für User kann auch der Zugriff verweigert werden, was in der Praxis leider auch vorkommt und besonders problematisch ist, wenn beispielsweise der Administrator oder der Backup-User betroffen ist.

Darüber hinaus gibt es noch die folgenden erweiterten Berechtigungen:

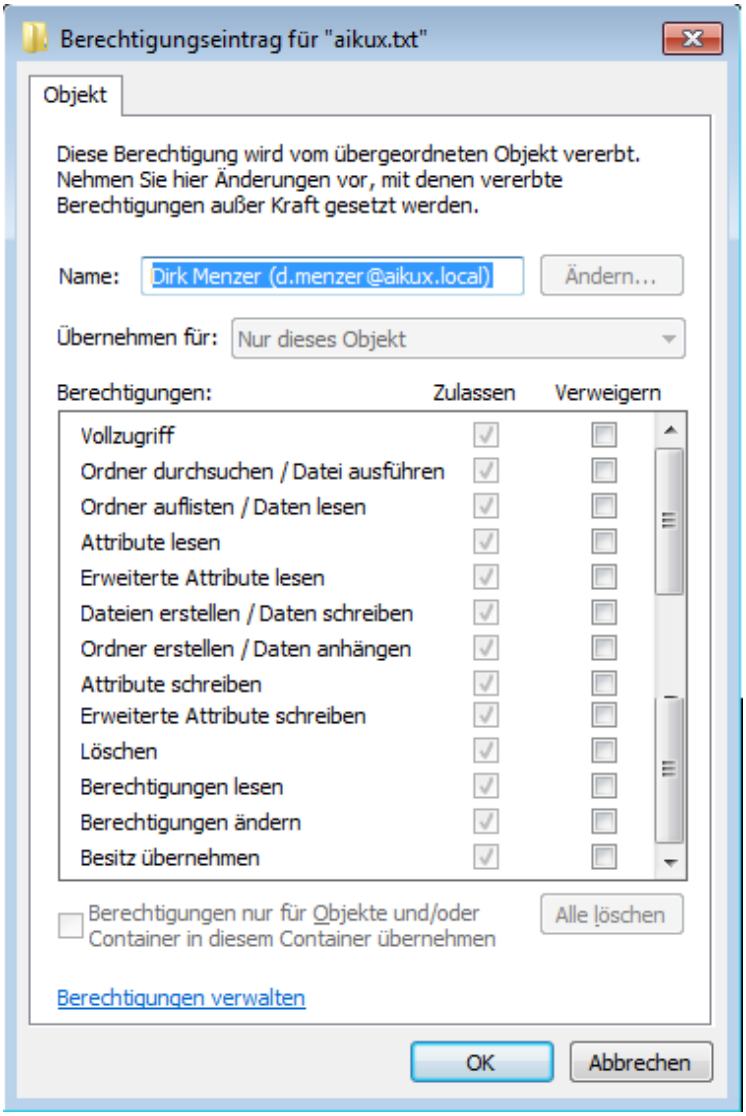

Abbildung 3: Erweiterte Berechtigungen

- **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 einer Datei oder einem Ordner zugewiesenen Berechtigungen
- **Berechtigungen ändern** – ermöglicht dem Benutzer das Ändern der einer Datei oder einem 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 einen Ordner immer ändern, unabhängig von den für die Datei oder den Ordner festgelegten Berechtigungen

Die speziellen Berechtigungen sollte man allerdings, genau wie auch das Verweigern von Berechtigungen, nur in Sonderfällen benutzen. Ein Verweigern ist unter normalen Umständen nicht notwendig, da bei einer durchdachten Verzeichnisstruktur die User auch nur dort Zugriff haben, wo sie ihn benötigen. Wenn man in Versuchung gerät, auf ein Verzeichnis einem Benutzer oder einer Gruppe den Zugriff zu verweigern, sollte man darüber nachdenken, die Vererbung zu unterbrechen und die Berechtigungen für dieses spezielle Verzeichnis neu zu vergeben.

3. Vergabe der Berechtigungen auf dem Share

Ein Share ist wie eine Gartentür zu verstehen, die ein Haus mit einem eigenen Schließsystem umschließt. Dort kann man das Recht setzen, dass man überhaupt erstmal in den Garten kommt. Die NTFS-Rechte sind dann die einzelnen Türen in dem Gebäude, die wiederum mit Schlössern versehen sind.

Hier empfiehlt sich mit differenzierten Rechten zu arbeiten. Z.B. Administratoren bekommen „Vollzugriff“ und Domänenbenutzer oder Authentifizierte Benutzer bekommen „Ändern“. Die Einschränkung der Rechte für bestimmte Benutzergruppen ist besonders wichtig, weil: Es ist möglich, dass man auf NTFS-Ebene mehr Rechte hat als gewünscht. Bildlich gesprochen ist die Tür über NTFS breiter als im Share. Wenn man jetzt aber durch die Gartentür will, ist diese zu eng und man kommt nicht mehr durch. Dies ist in folgendem Punkt besonders wichtig. Wenn ein User ein Verzeichnis erstellt, wird er auf NTFS-Ebene automatisch zum „Besitzer“ des Ordners und erhält dadurch gleich erweiterte Berechtigungen auf diesen Ordner. Es ist nämlich das Recht genau für diesen Ordner die Berechtigungen ändern zu können. Aber genau das will man in den meisten Fällen nicht. Wenn ein User versucht die Rechte zu ändern, würde das das NTFS-Recht zulassen, aber die „Ändern“ Rechte auf dem Share würde dies verhindern. Das ist ein Trick um sich lästige Änderungen zu ersparen!!!

4. Vergabe der Berechtigungen im Filesystem

Wie eingangs erwähnt, sollte man die Berechtigungen so „flach“ wie möglich gestalten, um eine gewisse Transparenz zu ermöglichen. Man kann die Berechtigungen sowohl auf Ordner als auch auf Dateien vergeben, wodurch ein Filesystem beliebig komplex werden kann. Die Vergabe der Berechtigungen erfolgt in der Regel durch AD-Gruppen (Active Directory Gruppen), damit zentral administriert werden kann.

4.1. Vergabe auf Ordner oder auf Dateien?

Die Vergabe der Berechtigungen bis auf Dateiebene ist nicht empfehlenswert, wenn man die Komplexität des Filesystems betrachtet. Man sollte also so weit möglich nur auf Ordner Berechtigungen vergeben, da bei einer Berechtigungsvergabe auch auf Dateien das gesamte Filesystem unter Umständen so unüberschaubar wird, dass es am Ende nicht mehr administrierbar ist.

4.2. A-G/U-DL-P Prinzip - Gruppen oder direkt berechtigen?

Berechtigungen „sollten“ in Microsoftumgebungen immer nach dem A-G-DL-P-Prinzip vergeben werden.

- A = Account
- G/U = Globale Domänen Gruppe/Universelle Domänengruppe -> hier werden die User drin geclustert; z.B. alle Mitarbeiter des Einkaufs
- DL = Domänenlokale Gruppe -> diese wird zur Vergabe der Berechtigungen im Filesystem genutzt; z.B. eine Gruppe für das Recht „Ändern“ mit dem Namen: „DL_V1_V2_V3_md“; „md“ steht dann für modify; diese Gruppe nimmt entweder die globale Gruppe oder im Ausnahmefall einzelne User auf.
- P = Permission

Man sollte sich angewöhnen, pro Berechtigung auch eine Gruppe im AD (Active Directory) anzulegen, z.B. „Verzeichnis_XY_ändern“ oder „Verzeichnis_AB_lesen“, die auch **nur** für diese Berechtigung benutzt wird, was die Berechtigungsvergabe wesentlich vereinfacht.

Da man nun überwiegend – außer bei der Einrichtung des Ordners – über Gruppen aus dem AD arbeitet, geht die Vergabe der Berechtigungen schneller und außerdem kann man einen Überblick über Berechtigungen bekommen, wenn man sich die Mitglieder der DL-Gruppe anschaut. Da sollten jetzt nur noch die drin sein, die Berechtigungen haben. Leider ist dies eins trügerische Annahme, da man sich unter Microsoft so nie sicher sein kann, wer tatsächlich berechtigt ist. Leider ist Microsoft an dieser Stelle extrem intransparent. Hier empfehlen wir die Nutzung von Drittanbieter Tools zur effektiven Darstellung von Berechtigungen.

HINWEIS: Leider hält sich noch stark eine Interpretation des A-G-DL-P-Prinzips aus NT Zeit. Deswegen hier noch mal der Hinweis zur Verwendung der Globalen Domänen Gruppe. Diese sollte tatsächlich eine Gruppe zur Clusterung der User nach einem Aufgabengebiet oder Organigramm sein (Z.B. Einkauf). In der Vergangenheit wurde die Domänen lokale

Gruppen oft gedoppelt: DL_V1_md wurde dann auch noch G_V1_md. Dies führt nur zur Verdoppelung der Gruppen und hat auch nach Microsoft eigener Aussage keinen praktischen Nutzen.

Man sollte also **NIE** einen User direkt auf einen Ordner berechtigen, da auch dadurch die Transparenz verloren geht und bei einer Löschung der User und dem Versäumnis, die Berechtigung zu entfernen, nur die SIDs der User auf dem Verzeichnis bleiben (tote SIDs):

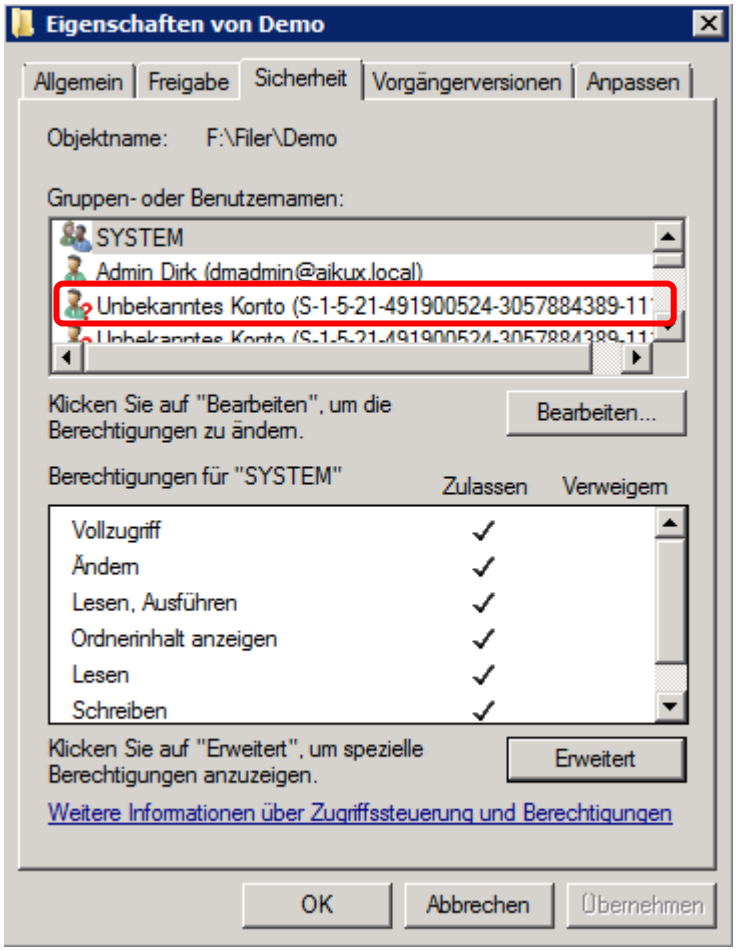

Abbildung 4: "Tote SIDs"

Was sich allerdings empfiehlt, ist das Anlegen von AD-Gruppen (z.B. Abteilungs- oder Projektgruppen), die auf mehrere Verzeichnisse berechtigt werden sollen, um nicht jedes Mal alle Benutzer einzeln in die entsprechenden Berechtigungsgruppen hinzufügen zu müssen.

4.3. Vererbung

Die Vererbung der Berechtigungen bedeutet, dass unterhalb eines Ordners die Berechtigungen, wie sie dort gesetzt sind, auch auf untere Ebenen übertragen werden. Das schließt natürlich nicht aus, in einer weiter unten gelegenen Ebene zusätzliche Berechtigungen hinzuzufügen.
Auch durch einen sinnvollen Einsatz der Vererbung kann erreicht werden, dass ein Kerberos-Token nicht übermäßig groß wird (s. 2.1.1). Man sollte in der obersten Ebene die Berechtigungen

so setzen, dass man sie gut nach unten hin durchvererben kann. Am besten nur Mindestberechtigungen auf root und wenn nötig die Berechtigungen erweitern. Und nur an denjenigen Stellen die Vererbung unterbrechen, an denen es notwendig ist, beispielsweise weil eine andere Berechtigungslage benötigt wird.

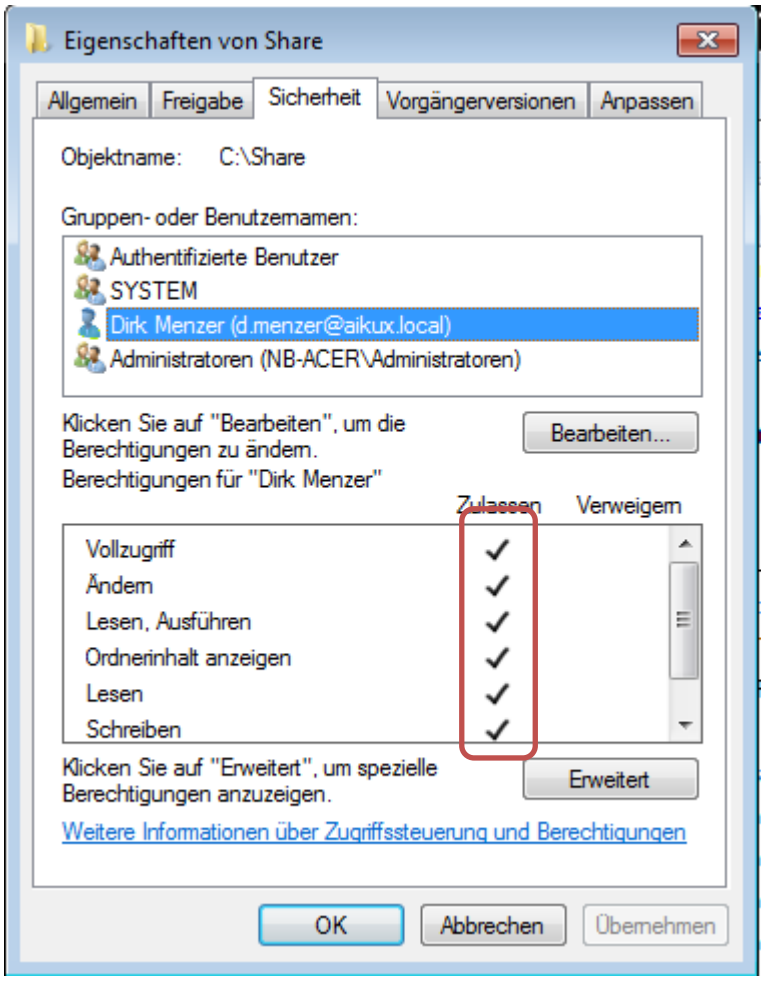

Abbildung 5: So sehen gesetzte Berechtigungen aus

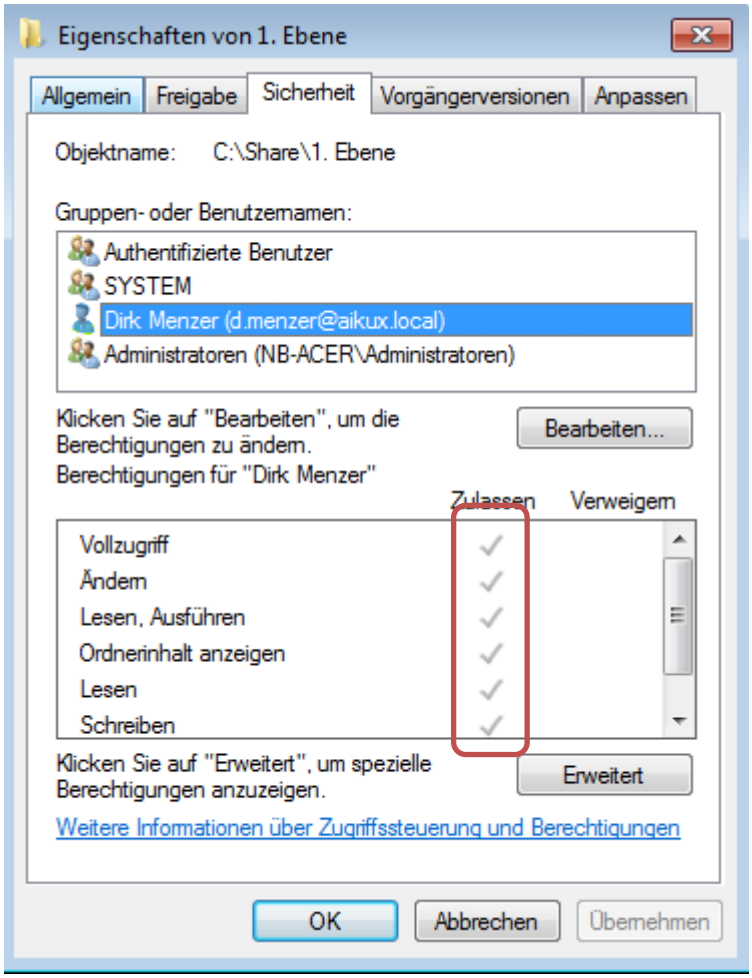

Abbildung 6: So sehen geerbte Berechtigungen aus

4.4. Listrechte

Listrechte sind Berechtigungen, die vergeben werden, um den Usern das Browsen durch die Verzeichnisse zu ermöglichen. Wenn ein User im Share einsteigt, möchte er sich auch bis in das für ihn relevante Verzeichnis „durchklicken“ können. Wenn man nun aber in der 4. Ebene eine Berechtigung setzt, kann er das nicht zwangsläufig. Hierzu vergibt man auf die darüber liegenden Verzeichnisse das Recht „Ordner auflisten“ nur für diesen Ordner:

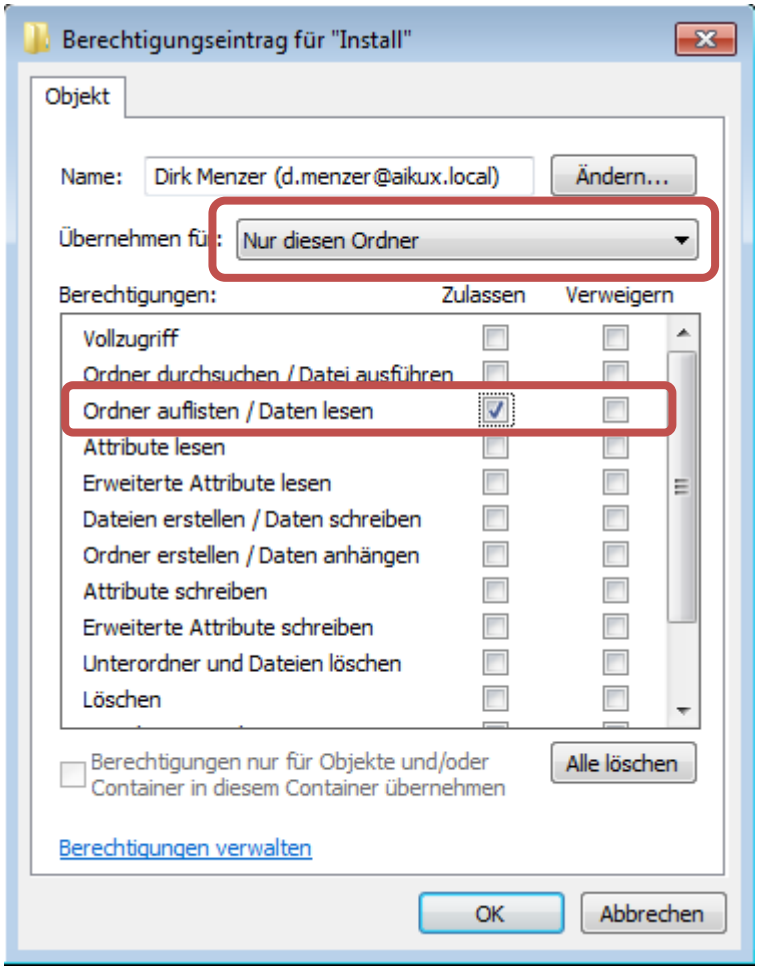

Abbildung 7: Listrechte vergeben

Zum Festlegen der Listrechte sind verschiedene Dinge zu beachten:

a. Wie viele Verzeichnisse mit geänderten Berechtigungen habe ich unterhalb des Shares und den darauf folgenden Ebenen?
b. Wie sieht die Gruppenzugehörigkeitslage bei den Usern aus? (Sind die User schon so in vielen verschiedenen Gruppen?)

Anhand dieser Begebenheiten muss man sich entscheiden, in welchen Ebenen man Listgruppen erzeugt und in welchen Ebenen man die Berechtigungsgruppen für die Listrechte benutzt.

Best Practice bei einer maximalen Berechtigungsvergabe bis zur 5. Verzeichnisebene ist, wenn man in der ersten und zweiten Verzeichnisebene Listgruppen einsetzt und in der 3. und 4. Ebene die Berechtigungsgruppen nutzt, siehe Bild:

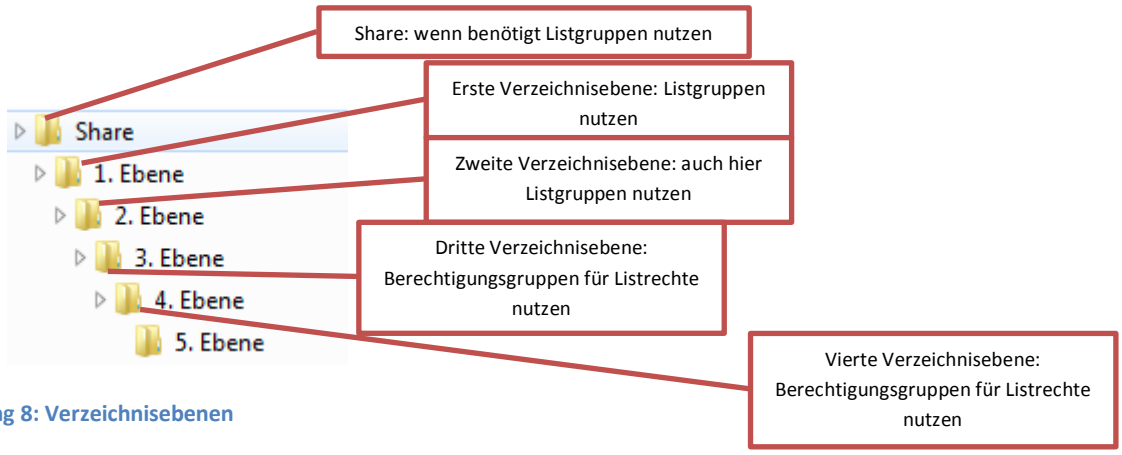

Abbildung 8: Verzeichnisebenen

Sofern man zum Beispiel nur die Berechtigungsgruppen benutzt ist hier zu beachten, dass in den obersten Ebenen eine Vielzahl an Gruppen in den Berechtigungen auftauchen, welche die Übersichtlichkeit stark reduzieren.
Im Umkehrschluss werden die Gruppenzugehörigkeiten der User stark erhöht, wenn man nur Listgruppen benutzt.

Merke: Die Listgruppenvergabe ist also individuell an jedes Filesystem und AD anzupassen.

5. Wie man vorgeht!

a. Herausfinden, wie groß das Kerberos-Token ist beziehungsweise in wie vielen Gruppen die User bereits Mitglied sind.
b. Herausfinden, wie viele Verzeichnisse mit geänderten Berechtigungen benötigt werden.
c. Entscheidung fällen, wie die Listrechte gesetzt werden sollen/müssen.
d. Setzen der Grundberechtigungen in der ersten Ebene und diese nach unten vererben.
e. Setzen der abweichenden Berechtigungen in den unteren Ebenen (von oben nach unten) und diese wieder nach unten vererben.
f. Setzen der Listgruppen bzw. Listberechtigungen.

6. Fazit

In kleineren Umgebungen können die Berechtigungen durchaus von Hand vergeben werden, in größeren ist dies nicht mehr sinnvoll umsetzbar, da eine komplexe Berechtigungsstruktur unweigerlich in einem nicht mehr überschaubaren Chaos endet.

Auch wenn man die Berechtigungsstruktur in Excel-Tabellen pflegt, weichen diese erfahrungsgemäß fast immer von der tatsächlichen Struktur ab, da immer wieder vergessen wird, eine schnell gemachte Änderung zu dokumentieren.

In größeren Umgebungen ist es also unverzichtbar, Tools zur Berechtigungsvergabe einzusetzen, welche die Berechtigungen vergeben und dokumentieren. Dazu kann man entweder Identity Management Systeme einsetzen oder 8MAN, was speziell für solche Aufgaben entworfen wurde.