NTFS-Berechtigungen

1. Authentifizierung (Wer greift zu?)

Access Token

Beim Einloggen eines Benutzers wird ein Access-Token erstellt.
Jeder vom Benutzer gestartete Prozess erhält eine Kopie dieses Access-Tokens.

Access Token
- SID des Benutzers - SIDs der Gruppen, in denen der Benutzer Mitglied ist - logon SID der Session - Liste von Privilegien des Benutzers und der Gruppen - SID des Besitzers - SID der primary group - ...

http://msdn.microsoft.com/en-us/library/aa374909%28VS.85%29.aspx

Windows Befehl: `whoami /all`

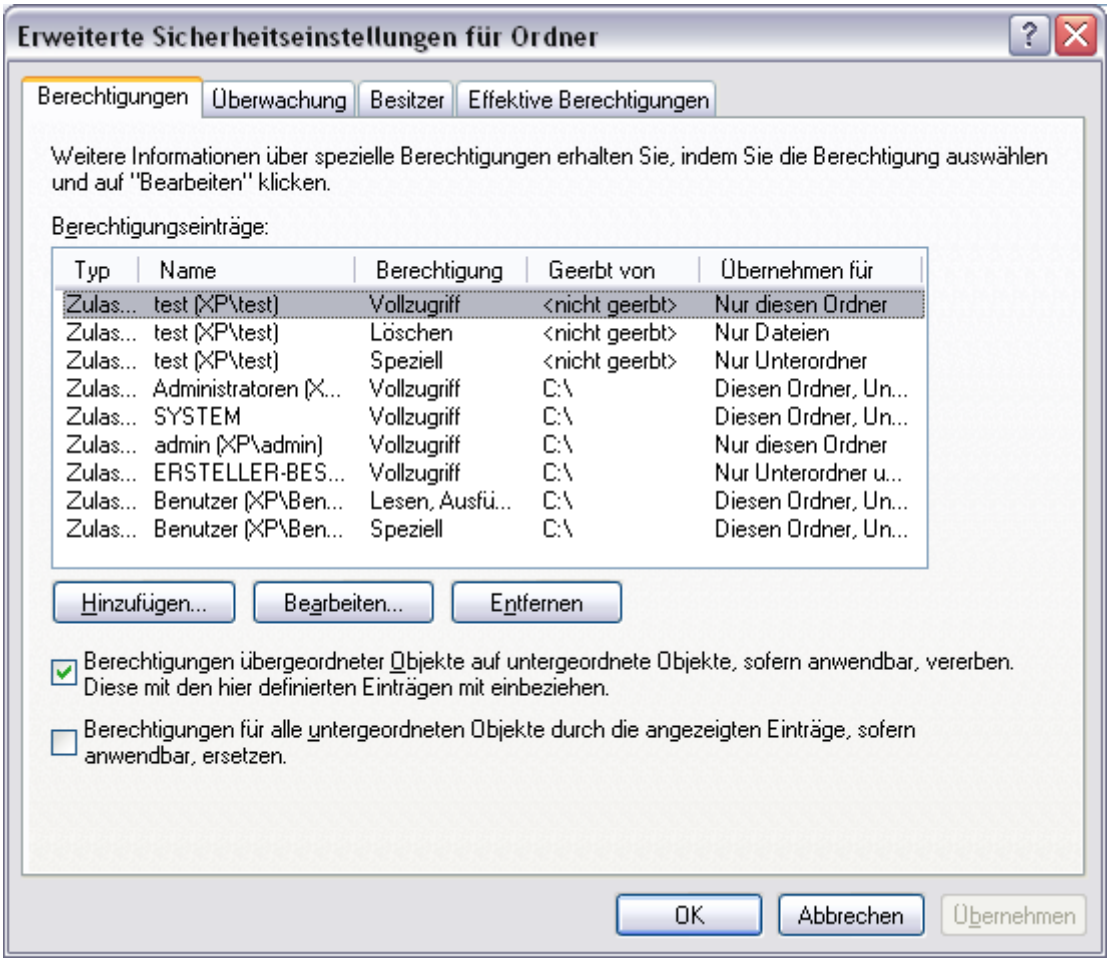
2. Autorisierung (Zuweisung von Zugriffsrechten)

Security Descriptor

Jedes sicherungsfähige Objekt (Laufwerk, Ordner, Datei, …)
kann einen Security-Descriptor haben, der festlegt, wer wie auf dieses Objekt zugreifen darf.

SD (Security Descriptor)

- SID des Besitzers
- DACL (Discretionary Access Control List)
  - ACE1
  - ACE2
  - ACE3
- DACL_PROTECTED (erben von oben?)
- SACL (System Access Control List)
  - ACE4
  - ACE5
  - ACE6
- SACL_PROTECTED (erben von oben?)
- …



http://msdn.microsoft.com/en-us/library/aa379563%28VS.85%29.aspx

Access Control Entry

ACE (Access Control Entry)

- Trustee (Benutzer oder Gruppe)
- ACEType (Allow / Deny)
- ACEFlags (vererben an)
  - Diesen Ordner
  - Unterordner
  - Dateien
- ACEMask (Rechte)
  - lesen
  - schreiben
  - ...