Benutzer und Berechtigungen

Checkpoints: Nach Studium dieses Dokuments und erledigten Aufgaben kann ich…

- ✓ lokaler von zentraler Benutzerverwaltung unterscheiden
- ✓ Dateien von Verzeichnissen unterscheiden
- ✓ Den Zweck von Benutzern und Gruppen erklären
- ✓ Dateizugriffe unterscheiden und Vererbung erklären
- ✓ Benutzer- und Berechtigungskonzepte erstellen und umsetzen
- ✓ den Begriff UNC-Pfad erklären und Freigaben erstellen bzw. nutzen

Nun geht's los:

- **Taschenrechner, Personalcomputer**: Sind Geräte und Daten **nicht gefährdet** (Lesen/Schreiben/Löschen etc.) und auch **nicht vernetzt**, kann auf die Benutzerverwaltung mit Vergabe von Zugriffsrechten verzichtet werden. Ohne eine solche Zugriffsregelung ist auch **kein User-Accounting** nötig. Sollten trotzdem mehrere Benutzer ein Gerät teilen, wie das z.B. bei einem Kopierautomaten der Fall ist, vergibt man so allerdings die Möglichkeit, die Benutzung verursachergerecht abzugelten.
- **PC-Sharing, IT-Umgebung**: Hier sieht das nun anders aus. Da möchte man seine Daten gerne **vor fremdem Zugriff schützen**. Darum werden **Zugriffsrechte** nötig. Dies bedingt aber auch eine **Benutzerverwaltung** (User-Accounting). Das heisst, man muss sich zuerst gegenüber dem System mit eigenem Benutzernamen und Passwort ausweisen (Authenifizierung). Diese Massnahme ist erst recht unverzichtbar, wenn das Gerät zusätzlich an ein Netzwerk angeschlossen ist, weil dadurch ein zusätzliches Gefährdungsrisiko von ausserhalb der Organisation besteht.

1. Benutzergruppen bilden

In professionellen IT-Umgebungen werden die Zugriffrechte nicht pro Benutzer, sondern **pro Gruppe geregelt**. Damit wird die **Benutzeradministration erheblich vereinfacht**, weil neue Benutzer durch Hinzufügen in die entsprechende Gruppe sofort alle für diese Gruppe notwendigen Berechtigungen erhalten.

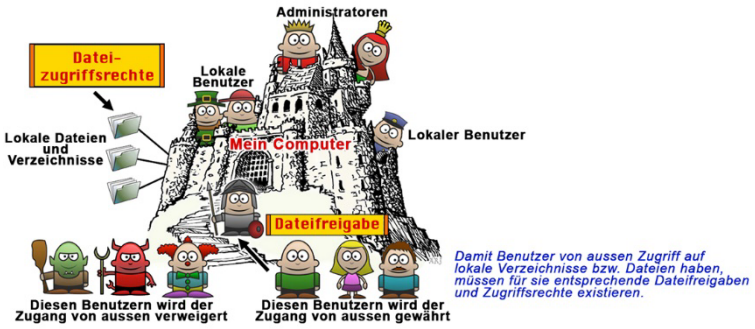
2. Lokale versus zentrale Benutzerverwaltung

- **Lokale Benutzerverwaltung**: Jeder PC bzw. das darauf installierte Betriebssystem verwaltet die Benutzer selbst. Dass bedeutet, dass der Felix Muster auf dem PC1 aus Sicht des Betriebssystems nicht derselbe ist, wie der aus biologischer Sicht selbige Felix Muster auf dem PC2. Das hat z.B. Auswirkungen bei den Berechtigungen und Freigaben. Will man Freigaben auf einem fremden PC nutzen, muss man dort einen Account besitzen. Beim Verbindungsaufbau zur Nutzung einer Dateifreigabe wird dies vom System jeweils überprüft. In der Praxis ist es so, dass die Anmeldung am fremden System nur einmal erfolgen muss. Danach kann sich das System an ihr "Privileg" "erinnern" und verzichtet auf eine erneute User/Passwort-Abfrage.

- **Zentrale Benutzerverwaltung**: In Firmen, Schulen etc., wo **Ressourcen gemeinsam genutzt** werden sollen, ist eine lokale Benutzerverwaltung zu umständlich. Dieser Dienst soll **innerhalb einer Domäne** zentral angeboten werden. Somit braucht man sich am System nur einmal anzumelden und kann anschliessend alle angebotenen Ressourcen, im Rahmen seiner Kompetenzen/Berechtigungen nutzen. Der Account wird also zentral auf einem Verwaltungsserver angelegt. Somit kann ich mit demselben Benutzeraccount auch jeden dieser Verwaltungsdomäne angeschlossene PC nutzen. Dieser Verwaltungsdienst nennt man allgemein **Directory-Services** und bei Microsoft-Windows **ActivDirectory**.

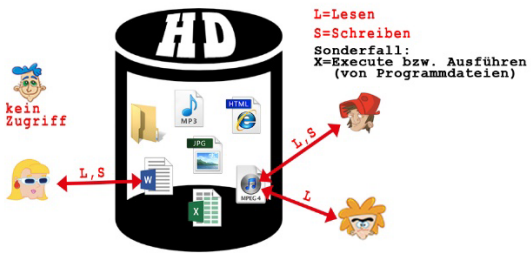
3. Datenzugriff Intern und von Extern

Der Dateizugriff für lokale Benutzer ist über die Zugriffsrechte geregelt. Für externe Benutzer existiert noch zusätzlich eine Hürde, nämlich die **Dateifreigabe**:



4. Zugriff auf Dateien und Verzeichnisse

Es kann auf Daten lesend und schreibend zugegriffen werden. Wobei die Dateien in einer baumartigen Verzeichnisstruktur abgelegt sind. (Verzeichnis oder Directory und Datei oder File)



5. Zugriffsrechte am Beispiel von UNIX/LINUX

Auf das wird zugegriffen: (Die Benutzer dürfen gemäss erteilten Berechtigungen auf Dateien oder Verzeichnisse zugreifen)

- **File**: Datei wie z.B. Text, Bild, Ton, Film, Programm, Tabelle …
- **Directory**: Verzeichnis als Auflistung der Dateien. *Das Directory ist strenggenommen auch ein File: Das Leserecht auf ein Verzeichnis bedeutet, dass man berechtigt ist, den Verzeichnisinhalt zu lesen bzw. aufzulisten. Schreibrechte auf einem Verzeichnis wiederum bedeutet, dass man am Verzeichnis Änderungen vornehmen darf, wie z.B. darin eine neue Datei/Verzeichnis erstellen, es umzubenennen oder gar zu löschen.*

Es werden die drei folgenden Zugriffsarten auf Verzeichnisse bzw. Dateien unterschieden:

- **READ**: Lesezugriff, Datei lesen, Bild anschauen, Ton hören …
- **WRITE**: Schreibzugriff, Text schreiben, Bild erstellen …
- **EXECUTE**: Ausführender Zugriff, Ausführrechte für ein Programm wie z.B. word.exe oder ein Batchfile)

Wobei diese drei Benutzerkreise existieren:

- **Owner**: Benutzer oder Eigentümer der Datei/Verzeichnis)
- **Group**: Gruppe oder Eigentümergruppe der Datei/Verzeichnis)
- **Other**: Die anderen oder der Rest der Welt

Nachteil dieses Systems: Es kann nur eine Person oder Gruppe Eigentümer sein. Alle anderen gelten als «Other» oder «Rest der Welt». (Dieser Nachteil wird mit ACL behoben.)

5.1 Benutzerrechte mit chmod ändern

Um Berechtigungen mit chmod, chown oder chgrp zu ändern, muss man am Verzeichnis, in dem sich das File befindet, die entsprechenden Rechte besitzen.
So ändert man die Benutzerrechte mit dem UNIX-Befehl «chmod»:

Die Berechtigung wird mit 9 Bit, aufgeteilt in 3-er Gruppen angegeben. Die erste Gruppe bezieht sich auf den **Owner**, die zweite auf die **Gruppe** und die dritte auf **Other**.

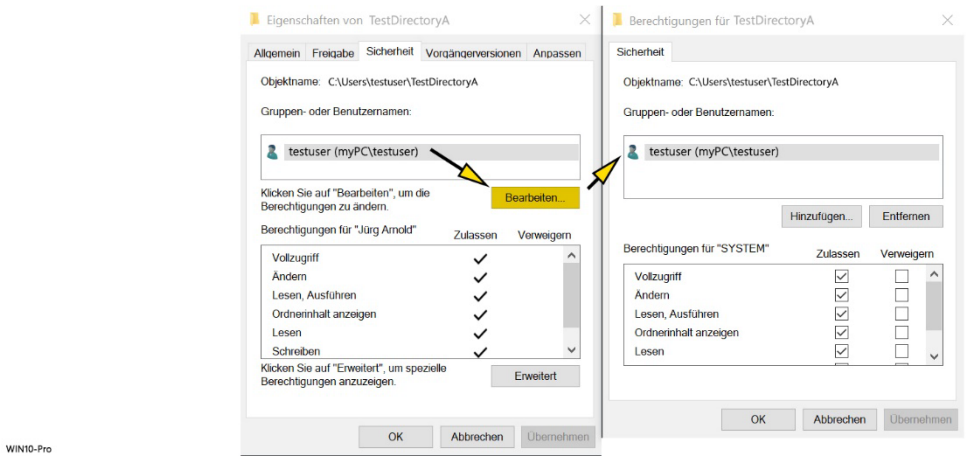
Zugriffsrechte unter UNIX

r w x	r w x	r w x	Zugriffsart
4 2 1	4 2 1	4 2 1	Wertigkeit der Bit-Stelle bei gesetztem Bit
Owner	Group	Others	Fokus oder Benutzerklasse

6. Sicherheitseinstellungen bei Microsoft-Windows

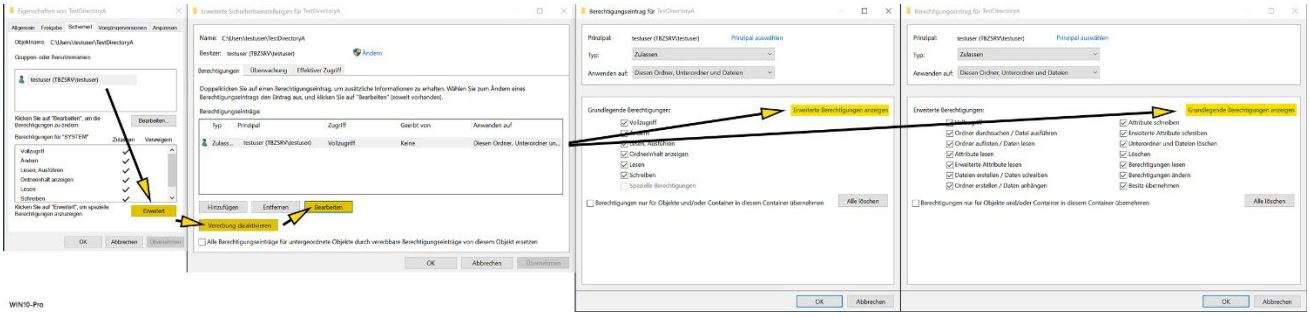
Obwohl auf Dateien und Ordner nur lesend, schreibend oder ausführend zugegriffen werden kann, wird in Microsoft noch etwas detaillierter unterschieden. Und zwar in den **beschränkten Sicherheitseinstellungen** und in den **erweiterten Sicherheitseinstellungen**. Ausserdem wird jeder Datei und Verzeichnis ein Zugriffskontrolldeskriptor zugeordnet, der eine ACL enthalten kann. Zu beachten: Um Berechtigungen anzupassen bzw. zu ergänzen, muss zuerst die **Vererbung** unterbrochen bzw. deaktiviert werden.

6.1 Die beschränkte Sicherheitseinstellung bei Microsoft-Windows



- **Lesen**: Nur Leserechte. Dateiausführung & Verzeichnisdurchsuchung nicht erlaubt.
- **Schreiben**: Nur schreibender Zugriff. Dateiausführung & Verzeichnisdurchsuchung nicht erlaubt. Setzen von Datei/Verzeichnis-Attributen erlaubt. Nur Leserechte auf Berechtigungen von Dateien/Verzeichnissen.
- **Lesen, Ausführen**: Objektänderungen (inkl. untergeordneten) nicht erlaubt. Leserecht für alle Attribute & Inhalte.
- **Ordnerinhalt auflisten**: Auf Verzeichnisse bezogen: Gleich wie „Lesen, Ausführen“. Lesen/Durchsuchen von Verzeichnis & Unterverzeichnissen. Lesen von Objekt-Attributen.
- **Ändern**: Änderungen & Löschen des Objekts. Ändern der Berechtigungen & Besitzübernahme nicht erlaubt. Kein Löschen von untergeordneten Objekten. Leserecht auf alle Objektoptionen.
- **Vollzugriff**: Alle Rechte auf Objekt und untergeordnetem Objekte. Lesen/Schreiben/Löschen/Modifizieren/Besitzübernahme

6.2 Die erweiterten Sicherheitseinstellungen bei Microsoft Windows

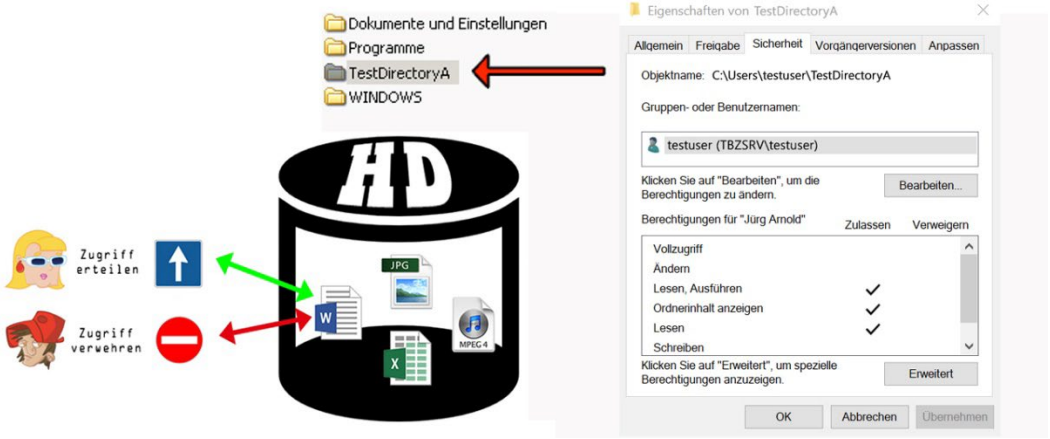


6.3 Beschränkte Sicherheitseinstellung versus erweiterte Sicherheitseinstellungen

Beschränkte Sicherheitseinstellungen	Vollzugriff	Ändern	Lesen & Ausführen	Ordnerinhalt auflisten	Lesen	Schreiben
Erweiterte Sicherheitseinstellungen						
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
Untergeordnete Ordner 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

7. Zulassen oder Verweigern?

Windows bietet für das Setzen der Zugriffsberechtigung zwei Möglichkeiten:



- «**Zulassen**» bedeutet, das darf dieser Benutzer tun
- «**Verweigern**» bedeutet, das darf dieser Benutzer nicht tun.
  «**Verweigern**» **hat höhere Priorität als** «**Zulassen**». Ist ein Benutzer Mitglied von zwei unterschiedlichen Gruppen, von der die eine zugelassenen Zugriff auf eine Datei hat und die andere verweigerten Zugriff, hat dieser Benutzer im Endeffekt keinen Zugriff auf diese Datei. Darum im Normalfall auf die Option «Verweigern» verzichten. Wenn die Zugriffsberechtigung nicht zugelassen wird, d.h. kein Häkchen (Checkmark) bei «Zulassen» gesetzt ist, wird dieses Zugriffsrecht auch nicht gewährt. Es braucht dazu kein spezielles «Verweigern».

8. Zugriffsrechte bei Microsoft-Windows in der Praxis

- **Zugriffsrechte unter WIN**: Die Zugriffsrechte unter MS-WINDOWS findet man in den «Dateieigenschaften» unter der Rubrik «Sicherheit».

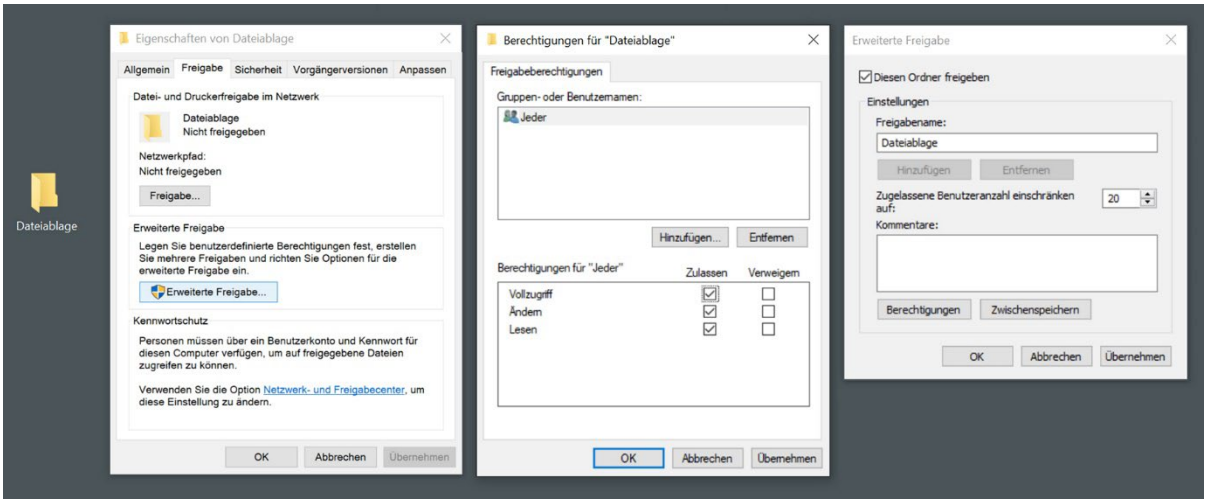
- **Vererbung** von Zugriffsrechten: Berechtigungen werden standardmässig an die untere Hierarchieebene vererbt. Das heisst, dass im Unterverzeichnis dieselben Zugriffsrechte gelten, wie im Übergeordneten. Will man diese Vererbungskette aufbrechen, muss man bei WINDOWS in den erweiterten Sicherheitseinstellungen die «Vererbbaren Berechtigungen des übergeordneten Objekts» ausschliessen. Danach hat man die Möglichkeit, die übergeordneten Berechtigungen zu kopieren oder zu entfernen.

- **Freigabe**: Externen Benutzern können sie Verzeichnisse über die Dateifreigabe zur Verfügung stellen. Dazu müssen sie die Eigenschaften des Verzeichnis aufrufen und in den Freigaben die «Erweiterte Freigabe» wählen. Danach geben sie diesen Ordner frei, indem sie einen geeigneten Freigabenamen wählen und die Berechtigungen vergeben. In unserem Fall ist es OK, wenn sie dem Benutzer «Jeder» Lesen und Ändern erlauben. Nun kann zwar jeder Benutzer, der auf dem System eingetragen ist, die Freigabe wählen, aber nur derjenige Benutzer, der auch die entsprechenden Zugriffsrechte hat, kann weiteres tun. (Zugriffsrechte siehe Dateieigenschaften-Sicherheit)

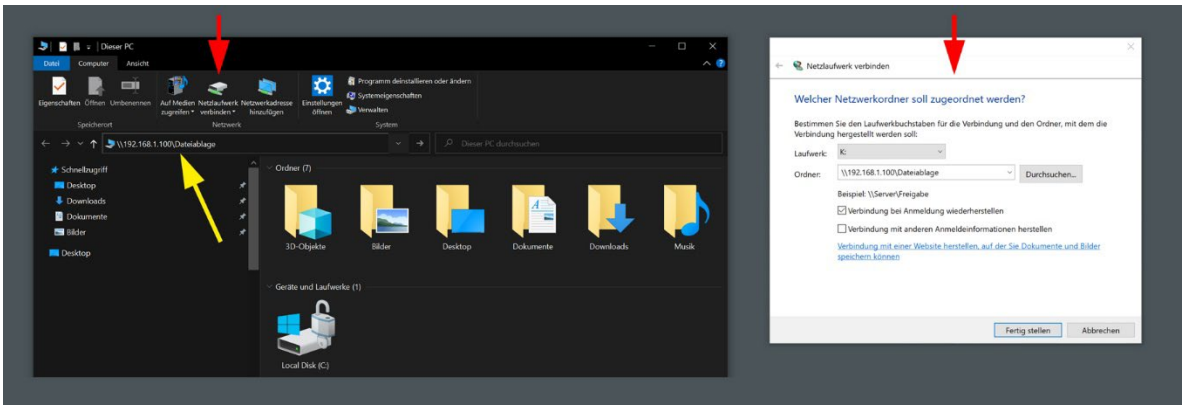
- **UNC-Pfad**: (**U**nified **N**aming **C**onvention) Dies ist ein Standard zur Bezeichnung von Netzwerkadressen in der Form:
  - \\Hostname\Freigabename
  - \\IP-Adresse\Freigabename
  - \\FQDN\Freigabename

    Hinweis: Der FQDN oder Full Qualified Domain Name wie z.B. pc01.tbz.local. muss von einem DNS-Server in eine IP-Adresse aufgelöst werden. Somit muss erstens ein DNS-Server existieren und zweitens die Domäne (tbz.local.) und auch der Host (pc01) dort bekannt sein.

    Der UNC-Pfad wird z.B. beim Verbinden von Netzlaufwerken angegeben.



- **Freigabe nutzen**: Windows-Explorer öffnen (Windows-Taste und «E»-Taste) und in der Adresszeile den UNC-Pfad der Freigabe eingeben. Anschliessend muss man sich gegenüber dem dateifreigebenden System mit einem dortigen lokalen User authentifizieren.



- **Netzlaufwerk verbinden / Freigabe einbinden**: Windows-Explorer öffnen (Windows-Taste und «E»-Taste) und im Menübereich «Netzlaufwerk verbinden» wählen. Damit können sie dem freigegebenen Netzwerkordner einen Laufwerksbuchstaben zuweisen. Wenn die entsprechende Checkbox angewählt ist, wird die Verbindung bei erneuter Anmeldung sogar wiederhergestellt. Wenn eine Netzlaufwerkverbindung zum ersten Mal erstellt wird, muss man sich gegenüber dem dateifreigebenden System mit einem dortigen lokalen User authentifizieren. (Dies ist im Sinne einer lokalen Benutzerverwaltung zu verstehen. Zentrale Verwaltungskonzepte sog. Directory Services bzw. Windows ActivDirectory werden im späteren Verlauf dieses Dokuments behandelt.)

- **Umstellen des Anmeldefensters**: Sobald mehrere Benutzer im System erfasst sind, wird das Standardverfahren beim Einloggen etwas mühsam. Unter Standardverfahren ist gemeint, dass die Benutzer als Benutzersymbole im Anmeldefenster angezeigt werden. In den Sicherheitseinstellungen (secpol.msc) kann das Anmeldefenster dahin geändert werden, dass anstelle der Benutzersymbole nun eine Eingabezeile «Benutzername» angezeigt wird: Sicherheitseinstellungen / Lokale Richtlinien / Sicherheitsoptionen / Interaktive Anmeldung: Letzten Benutzernamen nicht anzeigen AKTIVIEREN

- **Windows Arbeitsgruppen**: Um Dateien über das Netzwerk zwischen WIN-PCs auszutauschen, müssen die Geräte logisch miteinander verknüpft werden. WIN kennt dafür zwei verschiedene Methoden: Der Betrieb einer Domäne mit zentraler Verwaltung (ActivDirectory) oder die sogenannte Arbeitsgruppe. (Auf Domänen und AD wird hier nicht näher eingegangen.)

  Durch das Zuweisen der PCs zu einer oder mehrere Arbeitsgruppen werden logische Verbünde hergestellt. Mittels Freigaben können dann die PCs innerhalb einer Arbeitsgruppe Dateien austauschen oder auch einen gemeinsamen Drucker verwenden. Die Einrichtung von Arbeitsgruppen und Freigaben erfolgt im Gegensatz zu einer Domäne dezentral auf jedem Rechner einzeln. Voraussetzungen für den Betrieb von Arbeitsgruppen: Die PC's müssen sich im selben Subnetz befinden und den selben Arbeitsgruppennamen aufweisen .

9. Benutzer und Berechtigungskonzept erstellen

Die Planungsphase soll die Erstellung eines Benutzer und Berechtigungskonzept gemäss Vorgaben im Pflichtenheft beinhalten. In einer tabellenartigen Darstellung wird festgehalten, wer welche Rechte im Netzwerk besitzt. Es geht um Lese- bzw. Schreibrechte in Verzeichnissen und bei Dateien.

Folgendes muss zuerst abgeklärt werden (I wie Informieren von IPERKA):

- Welche **Personen** erhalten einen Zugang zum System?
- Welche **Gruppen** sollen erstellt werden? Bilden sie Gruppen und weisen sie die Benutzer den korrekten Gruppe zu. Erteilen Sie Zugriffsrechte auf Ordner und Dateien wenn immer möglich auf Gruppenebene und nur im Ausnahmefall an einzelne Benutzer. Mit diesen Massnahmen reduzieren sie den Administrationsaufwand bei neueintretenden, ausscheidenden und funktionswechselnden Mitarbeitern in ihrer Firma wesentlich.
- **Welche Benutzer** gehören **in welche Gruppen**? Benutzer können übrigens mehreren Gruppen angehören.
- **Namenskonzept** für Benutzernamen und Gruppennamen. Darunter gehört etwa die Bestimmung der maximalen Namenslänge (Max. Anzahl Charakters), der Umgang mit Umlauten und Spezialzeichen (Verzicht auf ö, ä, ü, é, è, à, etc.), das Vorgehen bei Namensvettern (Hans Meier1, Hans Meier2) etc.
- **Organisation** und Benennung der **Dateiablagen**:
    - Wer hat auf welche Dateien und Verzeichnisse welche **Zugriffsrechte**. D.h.: Wer darf in welchem Verzeichnis schreiben, wer darf lesen?
    - Welche Informationen unterstehen dem **Datenschutz** und welche Daten sind vertraulich?
    - Wer darf von ausserhalb der Systemgrenze welche Ressourcen nutzen? (**Dateifreigaben** und **Druckerfreigaben**)

Benutzer- und Gruppenmatrix (Beispiel)

Gruppen	Mitglieder
Mitarbeiter (MA)	Alle unten aufgeführten Personen (= Alle, die in diesem Betrieb einen Account brauchen)
Administratoren	admin, admin_stv, …
Geschäftsleitung (GL)	GL_1, GL_2, GL_3
Gruppe A (Gr. A)	Mitarbeiter_1, Mitarbeiter_5, Mitarbeiter_6
Gruppe B (Gr. B)	Mitarbeiter_2, Mitarbeiter_4, Mitarbeiter_7, Mitarbeiter_8, Mitarbeiter_10
Gruppe C (Gr. C)	Mitarbeiter_3, Mitarbeiter_9

Verzeichnis- und Berechtigungsmatrix (Beispiel)

Pfad \ Benutzerkreis	Beschreibung	Admins	GL	Gr. A	Gr. B	Gr. C	MA	User
\\Comp\Wartung	Updates, etc.	F						
\\Comp\Vorlagen	Vorlagen	F	C				R	
\\Comp\Transfer	Austausch	F					C	
\\Comp\Verz_2\Subdir_1	Gruppendaten	F	R	C				
\\Comp\Verz_2\Subdir_2	Gruppendaten	F	R		C			
\\Comp\Verz_3\Subdir_1	Gruppendaten	F	R			C		
\\Comp\Home		F					R	
\\Comp\Home\%username%	Persönliches Verzeichnis	F						C

Lese-Berechtigung:	R (READ)	Schreib-/Lese-Berechtigung:	C (CHANGE)	Vollzugriff:	F (FULL)

11. Neuer Harddisk in Betrieb nehmen (WIN)

Ausser bei Hot-Swap fähigen RAID-Systemen muss ein **Harddisk-Tausch** oder eine Harddisk-Erweiterung bei **ausgeschaltetem Rechner** erfolgen. Nach dem Booten des Rechners werden folgende Schritte in der Computerverwaltung unter Datenträgerverwaltung (Konsolenaufruf diskmgmt.msc) nötig:

- Datenträger initialisieren
- Auf Datenträger neue Partition erstellen
- Festlegen ob primäre oder erweiterte Partition
- Partitionsgrösse in MB angeben
- Laufwerksbuchstabe zuweisen oder leeren Ordner als «Mountpoint» bereitstellen
- Dateisystem festlegen. Bei WIN vorzugsweise NTFS verwenden.
  Hinweis zu Dateisystem: Das bei Memorysticks weit verbreitete FAT-Dateisystem hat Einschränkungen bei der max. Dateigrösse (<4GB), der Partitionsgrösse und unterstützt zudem keine Zugriffsrechte. Dafür kann es von allen Betriebssystemen WIN, Linux, OSX etc. gelesen und beschrieben werden.
- Datenträger bzw. Partition formatieren

12. Harddiskpflege

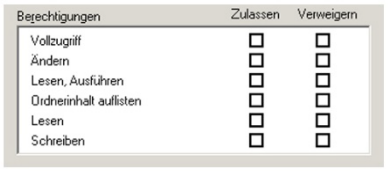
Bei magnetischen Speichermedien wie Harddisks soll man gelegentlich die Fragmentierung überprüfen (Verstreute Speicherung von logisch zusammengehörigen Datenblöcken des Dateisystems auf einem Datenträger) und allenfalls eine Defragmentierung durchführen. Dies ist bei SSD's (Solid-State-Disks) nicht nötig und wegen der begrenzten Anzahl von Schreibzyklen sogar kontraproduktiv.

10. Aufgaben zu Microsofts Sicherheitseinstellungen

1. **"Beschränkte Sicherheitseinstellung"**
   Unter welcher Bezeichnung/Benennung werden bei den beschränkte Sicherheitseinstellungen von Microsoft die folgenden Zugriffsberechtigungen zusammengefasst?

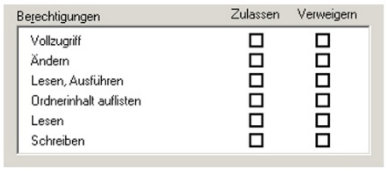
   a. Alle Rechte auf Objekt und untergeordnetem Objekte. Lesen / Schreiben / Löschen / Modifizieren / Besitzübernahme
   b. Objektänderungen (inkl. untergeordneten) nicht erlaubt. Leserecht für alle Attribute & Inhalte.
   c. Nur Leserechte. Dateiausführung & Verzeichnisdurchsuchung nicht erlaubt.
   d. Auf Verzeichnisse bezogen: Gleich wie „Lesen, Ausführen“. Lesen/Durchsuchen von Verzeichnis & Unterverzeichnissen. Lesen von Objekt-Attributen.
   e. Nur schreibender Zugriff. Dateiausführung & Verzeichnisdurchsuchung nicht erlaubt. Setzen von Datei/Verzeichnis-Attributen erlaubt. Nur Leserechte auf Berechtigungen von Dateien/Verzeichnissen.
   f. Änderungen & Löschen des Objekts Ändern der Berechtigungen & Besitzübernahme nicht erlaubt Kein Löschen von untergeordneten Objekten. Leserecht auf alle Objektoptionen.

2. **"Lesen/Schreiben/Kein Zugriff"**



Markiere die Felder für allgemeines «Schreiben (S)»

Markiere die Felder für allgemeines «Lesen (L)»



Markiere die Felder für «Kein Zugriff (X)»

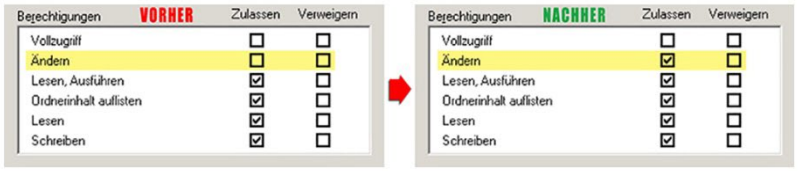
3. **"Lesen/Ausführen"**

Worin unterscheiden sich die Rechte bei zusätzlichem Lesen/Ausführen?

Was trifft zu?

   a. Datei in Form eines Programms/Batch kann auch ausgeführt (Execute) werden
   b. Datei kann gelesen werden
   c. Datei wird vom System entfernt bzw. hinausgeführt
   d. Metadaten einer Datei werden angezeigt
   e. Keine Antwort richtig

4. **"Ändern"**

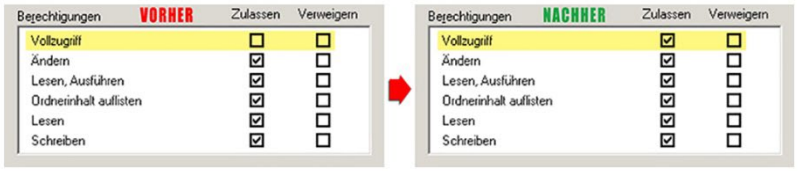


Worin unterscheiden sich die Rechte bei zusätzlichem Ändern?

Was trifft zu?

a. Daten im File können auch geändert werden
b. Zusätzliches Löschen des Objekts
c. Dateipfad ändern
d. Keine Antwort richtig

5. **"Vollzugriff"**

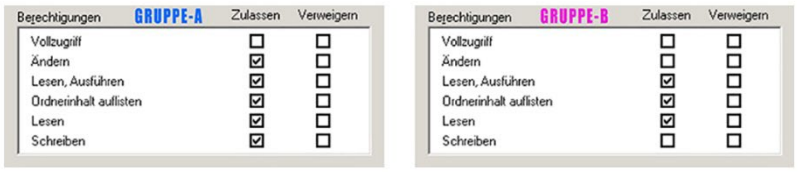


Worin unterscheiden sich die Rechte bei zusätzlichem Vollzugriff?

Was trifft zu?

a. Zusätzlich «Berechtigungen ändern»
b. Zusätzlich «Besitz übernehmen»
c. Zusätzlich «Untergeordnete Ordner/Dateien löschen»
d. Vollzugriff auf das ganze Dateisystem
e. Zusätzlich Administratorenrechte übernehmen, wenn nicht bereits als Administrator eingeloggt

6. **"Zulassen"**

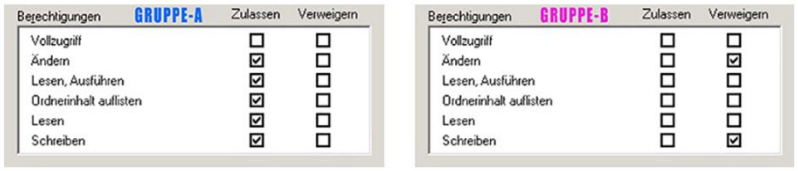


Herr Muster ist Mitglied von Gruppe-A und Gruppe-B. Welche Rechte besitzt er?

Was trifft zu?

a. Vollzugriff
b. Ändern
c. Lesen, Ausführen
d. Ordnerinhalt auflisten
e. Lesen
f. Schreiben

7. **"Verweigern"**



Frau Muster ist Mitglied von Gruppe-A und Gruppe-B. Welche Rechte besitzt sie?

Was trifft zu?

a. Vollzugriff
b. Ändern
c. Lesen, Ausführen
d. Ordnerinhalt auflisten
e. Lesen
f. Schreiben

8. **"Mehreren Gruppen angehören"**

Was trifft zu, wenn der Benutzer «testuser» die Berechtigungen auf sein Verzeichnis «TestDirectoryA» wie gezeigt ändert?

Was trifft zu?

a. «testuser» kann sein Verzeichnis nicht mehr ändern oder löschen
b. «testuser» kann sein Verzeichnis lesen
c. Es werden Administratorenrechte benötigt, um dem Benutzer «testuser» wieder Schreibzugriff auf sein Verzeichnis zu ermöglichen
d. Da das Verzeichnis «TestDirectoryA» vom Benutzer «testuser» erzeugt wurde, hat er grundsätzlich alle elementaren Rechte darauf

9. Eine umfangreichere **Praxisaufgabe** folgt in einem separaten Dokument!