ACL Konzept NEU 11.2016

Das Problem bei den ACLs ist immer die Übertragung über Inodelevel hinaus, und auch über die Maske selbst hinaus. Da dies ja nicht geht hier ein neues Konzept das genau dieses Problem umgeht. Funktionieren kann das nur wenn die Maske von Quelle und Ziel immer gleich ist.

Wir erstellen uns einen Ordner Dokumente1 in home und setzen hierfür die Rechte.

```
mkdir /home/Dokumente1
chgrp dokumente /home/Dokumente1
setfacl  -m group:dokumente:rwX,other:rwX /home/Dokumente1  # setzt die ACL
des Ordners
setfacl -d -m group:dokumente:rwX,other:rwX /home/Dokumente1  # setzt die
Default ACL des Ordners
chmod g+s /home/Dokumente1
chmod 770 /home/Dokumente1
```

Die Rechte sehen jetzt so aus:

```
getfacl /home/Dokumente1
# file: Dokumente1
# owner: root
# group: dokumente
# flags: -s-
user::rwx
group::rwx
group:dokumente:rwx
mask::rwx
other::---
default:user::rwx
default:group::rwx
default:group:dokumente:rwx
default:mask::rwx
default:other::rwx
```

Wie man sieht darf in diesem Ordner jeder Schreiben und lesen. Das ist aber kein Sicherheitsproblem da man Mitglied der Gruppe „Dokumente“ sein muss um überhaupt in dem Ordner zu gelangen. Wichtig ist hier bei „getfacl“, rwX zu schreiben und nicht rwx. Der Unterschied ist bei großem X nur die Auflistung des Ordnerinhaltes gewährt wird, was natürlich auch einem möglichem Schreiben im Ordner gleicht. Es gewährt aber keinesfalls „Ausführen“ von Dateien in diesem Ordner. Diese dürfen natürlich von jedem Benutzer gesetzt werden, aber es ist kein Standard bei neuen Dateien.

Problem mit grafische Programmen wie Dolphin

Dolphin regt sich hier bei jedem ACLbreich übergreifenden Kopieren oder Verschieben auf das die Rechte nicht geschrieben werden können. Das nervt. Um das ganze zu umgehen setzen wir die ACLs wie folgt:

```
mkdir /home/firmendaten
chown -R root:nogroup /home/firmendaten
find /home/firmendaten -type d -exec chmod 777 {} +
find /home/firmendaten -type f -exec chmod 666 {} +
setfacl -R -m other:rwX /home/firmendaten  # setzt die ACL des Ordners (-R
vor -m für recursiv)
setfacl -R -d -m other:rwX /home/firmendaten  # setzt die Default ACL des
Ordners  (-R vor -m für recursiv)
chmod 770 /home/firmendaten
chgrp firmendaten /home/firmendaten
```

```
/home/ getfacl firmendaten
# file: firmendaten
# owner: root
# group: firmendaten
user::rwx
group::rwx
other::---
default:user::rwx
default:group::rwx
default:other::rwx
```

Wir können die Gruppe getrost weglassen, da wir diese ja nur beim Eingang (spricht den Ordner) der ACL benötigen. Natürlich müssen alle anderen ACLbereiche (auch Homeverzeichnisse) so gesetzt sein. Damit bekommt man die Fehlermeldung in Dolphin nicht mehr. Sieht man sich den Inhalt an, irritiert dieser ein wenig. Passt aber definitiv zum Rechtesystem.

```
drwxrwxrwx+  4 root   nogroup    4096 Dez  2 20:36 Testordner
-rw-rw-rw-   1 root   nogroup  757681 Jul 11 08:35 Testdatei.txt
```

Neue Dateien werden mit der Gruppe und dem Eigentümer des Users angelegt.

Neue Homeverzeichnisse setzen

Dies ist nur möglich wenn sich im Homeverzeichnis keine Daten befinden. Hiervon sind versteckte Dateien unberührt.

```
chmod 777 /home/user
chmod 777 /home/user/*
setfacl -d -m other:rwX /home/user
setfacl -m other:rwX /home/user
setfacl -m other:rwX /home/user/*
setfacl -d -m other:rwX /home/user/*
chmod 700 /home/user
```