

## Hinweise zur Sicherheit

### Hinweise zur Sicherheit

#### Accounting

Aus Sicherheitsgründen ist (gemäß der [Benutzer-Ordnung](#)) Accounting aktiviert. Dies bedeutet, dass erfasst wird, welche Programme von einem Benutzer wann gestartet werden und wieviel Rechenleistung verbraucht wird.

#### Sichere Passwörter

Allen Benutzern des Computer Pools wird **dringend** geraten, ein sicheres Passwort zu verwenden. Das Passwort sollte **mindestens** 10 Zeichen lang sein und eine Mischung aus Kleinbuchstaben, Großbuchstaben, Sonderzeichen und Zahlen sein. Das Passwort sollte nicht für andere Accounts verwendet werden. Das Passwort sollte für andere schwer zu erraten sein und sollte daher nicht das eigene Geburtsdatum, der (Spitz-)Name der Freundin oder die Rasse des Haustieres sein.

Als gute Passwörter haben sich die Anfangsbuchstaben eines Satzes (z.B. eines Sprichwortes) erwiesen. Man wählt einen Satz, in diesem Beispiel "1 sicheres Passwort zu wählen ist eigentlich nicht schwer." und verwendet die Anfangsbuchstaben und Satzzeichen als Passwort, in diesem Beispiel "1sPzw=ens.". Auf diese Weise erhält man relativ sichere Passwörter, die gut zu merken sind. Dieses Passwort sollte man natürlich **nicht** verwenden.

#### Ausloggen und Bildschirm-Sperre

Wer den Rechner, an dem er arbeitet, verlässt oder aus den Augen lässt, sollte sich entweder ausloggen oder sollte den Bildschirm sperren. Bei KDE kann die Bildschirm-Sperre über das Symbol des blauen Vorhängeschlosses aktiviert werden. Um die Sperre aufzuheben gibt man auf Nachfrage sein Passwort ein.

#### Datei- und Verzeichnisrechte

Standardmäßig sind die Rechte auf das home-Verzeichnis so gesetzt, dass nur der Benutzer selbst in sein home-Verzeichnis schreiben darf, dass aber jeder den Inhalt des Verzeichnisses lesen kann. Wer das nicht will, kann seine Dateien entweder im Verzeichnis privat in seinem home-Verzeichnis ablegen, das standardmäßig nicht für andere Nutzer lesbar ist, oder er kann mit

```
chmod 700 ~
```

den anderen den Zugriff entziehen. Wer sich selbst die Rechte entzieht, kann sich nicht mehr einloggen.

Bis auf kleine Ausnahmen werden Verzeichnisse wie Dateien behandelt. Die Rechte auf einem Unix-System beziehen sich auf den Besitzer der Datei (u), die Gruppe (g), der er angehört, und den Rest der Welt (o). Sind alle drei Kategorien gemeint, kann man auch a verwenden. Für jede dieser drei Kategorien kann man getrennt das Recht zum Lesen (r), zum Schreiben (w) und zum Ausführen (x) festlegen. Wenn man ein Verzeichnis "ausführen" darf, bedeutet das, daß man in dieses Verzeichnis hineinwechseln darf. Das Schreibrecht von Dateien bezieht sich auf das Anlegen und Löschen von Dateien, sowie das Ändern von Dateirechten in diesem Verzeichnis.

`chmod o-r datei` entfernt also für alle außer dem Besitzer und Angehörigen der Gruppe die Leseberechtigung auf die Datei *datei*. `chmod a+x datei` gibt analog die Datei *datei* für alle zum Ausführen frei. `chmod g+w datei` erlaubt allen in der Gruppe das Schreiben der Datei *datei*.

Oft wird statt dieser textuellen Darstellung die oktale Darstellung der Zugriffsrechte verwendet. Hierbei entspricht 4 dem Leserecht, 2 dem Schreibrecht und 1 dem Recht, die Datei auszuführen. Die Rechte, die gesetzt sein sollen, werden - für die drei Kategorien getrennt - addiert. `chmod 640 datei` erlaubt also dem Besitzer der Datei *datei* das Lesen und Schreiben, Angehörigen der Gruppe nur Lesezugriff und allen anderen überhaupt keinen Zugriff.

Wird ein Verzeichnis neu erstellt, so erhält es als Rechte 755, also 777 (alle Rechte) abzüglich der umask von 022. Dateien erhalten 644 (666 minus 022), keiner hat also zunächst das Recht, sie auszuführen.

Um die aktuellen Zugriffsrechte festzustellen, kann man `ls -l datei` verwenden. Ein typischer Output ist `-rw-r--r-- 1 pkilian cip-pool 0 2005-05-11 13:37 datei`

Der erste - bedeutet dabei das es sich um eine reguläre Datei handelt. Bei einem Verzeichnis stünde d, bei einem Charakterdevice c, bei einem Blockdevice b, bei einem Softlink l und p bei einer named pipe.

Die darauffolgenden 9 Zeichen geben die Rechte des Besitzers, der Gruppe und der anderen an.

Die folgende Zahl gibt die Anzahl an Hardlinks auf diese Datei an.

Dann folgen der Benutzer, die Gruppe und die Dateigröße.

Als nächstes kommen Datum und Uhrzeit des letzten Schreibzugriffes.

Am Ende kommt der Dateiname.

Prinzipiell kann man auch den Besitzer oder die Gruppenzuordnung einer Datei ändern. Weitere Informationen dazu findet man in den Man-Pages `man chown` und `man chgrp`.

Zusätzlich zu den bisher genannten Rechten gibt es noch `set user ID` (4), `set group ID` (2) und `sticky` (1).

Das **set user ID** Bit (oft auch als `suid` bezeichnet) bedeutet bei ausführbaren Dateien, daß das Programm mit den Rechten des Besitzers, nicht mit denen des Aufrufenden gestartet wird. Das Setzen dieses Bits ist daher fast immer als Sicherheitsrisiko zu betrachten. Bei Verzeichnissen wird das Bit üblicherweise ignoriert.

Das **set group ID** Bit bedeutet für (ausführbare) Dateien, daß das Programm in der Gruppe des Besitzers und nicht in der Gruppe des Aufrufenden läuft. Bei Verzeichnissen hingegen sorgt es dafür, dass alle Dateien, die darin angelegt werden, der Gruppe gehören, der das Verzeichnis gehört.

Das **sticky bit** wird heutzutage bei Dateien ignoriert. Bei Verzeichnissen bewirkt es, dass Dateien innerhalb dieses Verzeichnisses nur vom Besitzer der Datei (und von `root`) gelöscht werden können und nicht von jedem, der Schreibrechte auf das Verzeichnis hat. Sinnvoll läßt sich dieses Bit vor allem bei systemweit schreibbaren Verzeichnissen wie `/tmp` verwenden.

Wenn man diese speziellen Bits nutzen möchte, addiert man die Werte, die man setzen möchte und gibt sie **vor** den Rechten für den Besitzer an. `chmod 4750 datei` erlaubt dem Benutzer also vollen Zugriff und erlaubt Mitgliedern der Gruppe das Lesen und Ausführen.

Außerdem ist die Datei `set user ID`, was auch in der Ausgabe von `ls -l datei` als

```
-rwsr-xr-x Zahl_der_Hardlinks Besitzer Gruppe Größe Datum datei
```

auftaucht (das hier fett markierte `s` statt dem üblichen `x`).

Über die hier erklärten Rechte hinaus gibt es noch die Möglichkeit ACLs (Access Control Lists) zu verwenden. Informationen dazu findet man unter z.B. unter `man acl` sowie unter `man setfacl` und `man getfacl`.