Wenn man in den Genuss kommen sollte, einen rsh-Server auf einem Rechner betreiben zu müssen, sollte man sich die folgenden Tipps zu Herzen nehmen.

Grundsätzliches

Achtung:

Es wird nicht empfohlen, einen rsh-Server zu betreiben. Die Gründe hierfür sind klar: Die Anmeldedaten, sowie alle andere Daten, die per r-Tools (rsh, rcp, rlogin, ...) übertragen werden, sind unverschlüsselt.

Die Tools, die man hierfür verwenden sollte sind SSH und SCP.

Aber trotz der Risiken haben die r-Tools auch Vorteile:

1. der rsh-Server ist ein Dienst, der über xinetd gestartet wird, d.h.
    1. der rsh-Server ist nicht ständig am Laufen (Performance-einbußen)
    2. Xinetd kann über die hosts-dateien gesteuert werden (Zugriffe)
2. die Passwortlose Authentifizierung ist relativ einfach einzurichten
3. Aufgrund er fehlenden Verschlüsselung sind r-Tools sehr schnell
4. r-Tools erzeugen nicht viel Last auf dem Serversystem (Verschlüsselung fehlt)

Absicherung

Die Zugriffssteuerung wird bei xinetd über die Dateien */etc/hosts.deny*, */etc/hosts.allow* und */etc/hosts.equiv* gesteuert. Dabei gilt: Durch die Datei */etc/hosts.deny* werden Zugriffe auf den eigenen Rechner gesperrt, sofern sie nicht durch */etc/hosts.allow* erlaubt werden.

Standardmäßig kann sich jeder nach der Installation auf dem Server per rsh einloggen. Dies ist eigendlich kein Beinbruch. Da aber rsh wegen der fehlenden Verschlüsselung sehr unsicher ist, sollte der Einsatz von rsh so weit wie möglich unterbunden werden.

Deshalb unterbinden wir grundsätzlich das einloggen auf dem Server mit folgender Zeile in der Datei */etc/hosts.allow*

hosts.allow

```
ALL : ALL
```

Jetzt ist der Server fürs Erste dicht. Jetzt kann man aber auch alle anderen Dienste vergessen, die über xinetd gestartet werden. Will man nur den rsh-Server schließen, ist folgende Zeile ausreichend:

hosts.allow

```
in.rlogind : ALL
```

Lockerung der Absicherung

Die bis jetzt erklärte Konfiguration (Wir installieren einen rsh-Server und blockieren alle Anfragen) macht noch nicht viel sinn. Jetzt müssen wir explizit die Rechner angeben, die Zugriff haben sollen.

Dies geschieht mit der folgenden Zeile in der Datei */etc/hosts.allow*

hosts.allow

```
in.rlogin : <IP-Adresse>
```

somit darf der Rechner mit <IP-Adresse> auf den rsh-Server zugreifen. Alle anderen werden weiterhin blockiert

Passwortloser Zugang

Wenn man jetzt schon soweit gekommen ist, kann man auch noch verschiedene Usern erlauben, Passwortlos auf das System zuzugreifen

Am einfachsten ist dies, wenn man in der Datei */etc/hosts.equiv* Ein Plus (+) eingibt. Dies heißt soviel wie: Jeder darf ohne Passwort zugreifen. Dies ist natürlich nicht im Sinne des Erfinders.

Will man auf den User test123 ohne Passwort zugreifen, so