SSH-Konfiguration

Die Grundkonfiguration des sshd Service ist nach einer Minimalinstallation von CentOS 7 aus Sicherheitsgünden den eigenen Bedürfnissen anzupassen:

Login mittels Benutzername/Passwort oder SSL-Key

Persönlich bevorzuge ich den Login mittels Benutzername/Passwort, da ich mich gerne von verschiedenen Geräten aus auf einem Server einlogge. Hierzu legen wir zunächst einen neuen Benutzer an und vergeben dann ein Passwort für diesen neuen Benutzer

```
adduser BENUTZERNAME
```

```
passwd BENUTZERNAME
```

Root-Login deaktivieren

Aus Sicherheitsgründen deaktivieren wir den direkten Root-ogin in der Datei `/etc/ssh/sshd_config` wie folgt. alt:

```
#PermitRootLogin yes
```

neu:

```
PermitRootLogin no
```

Nun noch den sshd neu starten mittels dem Befehl

```
service sshd restart
```

Ab sofort kann man sich nur noch als Benutzer per SSH einloggen und mittels des Befehls ***su*** root-Rechte erhalten.

SSH-Port ändern

Um unter CentOS 7 den SSH-Port zu verändern sind im groben 3 Schritte nötig. Die SSH-Config Datei verändern, die Firewall anpassen und schließlich noch einige SELinuxregeln abändern.

1. SSH-Config Dateien ändern

Unzählige automatisierte Scripte durchforsten das Internet nach Rechnern mit geöffnetem SSH auf

dem Standard-Port 22, um mittels Brute Force Attaken unbefugten Zugang zu erhalten. Deshalb sollte als erstes in der SSHd Config Datei `/etc/ssh/sshd_config` die Portnummer geändert werden. Darin ist eine auskommentierte Zeile mit ‚# Port 22' zu finden. Den Kommentar entfernen und die 22 durch die gewünschte Portnummer ersetzen. In meinem Beispiel der Port 1234. alt:

```
#Port 22
```

neu:

```
Port 1234
```

Das neu starten des sshd Dienstes geschieht erst nach Änderung an den SELinuxregeln, da sonst eine Fehlermeldung erscheint.

2. Firewallregeln anpassen

Neuen Port öffnen

```
firewall-cmd -–zone=public –-add-port=1234/tcp
```

Alten SSH-Port entfernen

```
firewall-cmd -–zone=public –-remove-port=22/tcp
```

Die Änderungen speichern und den Firewalldienst neu laden.

```
firewall-cmd –-runtime-to-permanent
firewall-cmd -–reload
```

3. SELinuxregeln abändern

Um den SSH-Port ändern zu können, müssen wir vorher noch ein Paket für die Verwaltung von SELinux installieren.

```
yum install policycoreutils-python
```

Danach können wir als letzten Schritt die SELinux-Regeln anpassen.

```
semanage port -a -t ssh_port_t -p tcp 1234
```

Nun können wir den SSH-Dienst neu starten

```
systemctl restart sshd.service
```