Teil II zur Systemsicherheit.

Wie im vorigen Artikel bereits beschrieben soll man relvante Dienste die nach aussen transportiert werden mit user-Rechten versehen um das System zu sichern.

Wenn man seine "Standard-Ports" nach aussen hin "verbiegt" kann man sein System noch weiter absichern.

Beispiel SSH:
Man kann den SSH-Port in der Datei /etc/ssh/sshd_config auf einen anderen als den Standard-Port 22 legen. Beispielsweise auf 4022.

Alle TCP-IP Ports über 1024 bis 65535 sind sogenannte "unpriveligierte" Ports.
Auf diesem Ports kann man Applikationen laufen lassen wie man möchte.

Wenn man also in der sshd_config die Portangabe von Standard 22 auf einen anderen port "anhebt" wird das System nach aussen unsichtbar, da auf dem Port 22 permanent gescannt und auch angegriffen wird.

Wenn man zusätzlich noch
AllowGroups users
DenyGroups root
DenyUsers root

unten anfügt dann wird das "root-Login" über ssh pauschal verboten.

Man muss sich dann zwar als User am System anmelden und auf der Konsole einmal su- mit Passwort eingeben. Das mag zwar im ersten Moment aufwändiger erscheinen aber man gewöhnt sich schnell daran sich zweimal anzumelden wenn man mal "root" werden muss.

Viel Spass beim ausprobieren.

euer Admin