Hier eine Beschreibung wie man SELinux einstezt.

In den meisten Foren (auch bei RedHat) heisst es: "Wenn Du ärger mit SELinux hast schalte es ab !"

Das ist völlig falsch. SELinux beitet die Möglichkeit das System zusätzlich zu schützen
und nur die benötigten Ports zu öffnen.

Hierbei benutzt man den firewalld von CentOS / Redhat und in diesem Beispiel den Webserver zu schützen,
da die www-Verzeichnisse in den SELinux-Kontext eingebunden werden.

RedHat / CentOS

```
firewall-cmd --zone=public --add-service={http,https} --permanent
firewall-cmd --zone=public --add-port=80/tcp --permanent
firewall-cmd --zone=public --add-port=443/tcp --permanent
firewall-cmd --zone=public --add-port=10000/tcp --permanent
firewall-cmd --zone=public --add-port=8080/tcp --permanent
firewall-cmd --reload
```

Selinux konfigurieren:

```
semanage fcontext -a -t cert_t "/var/www/(.*)/pki(/.*)?"
semanage fcontext -a -t http_script_exec_t "/var/www/(.*)/cgi-bin(/.+)?"
semanage fcontext -a -t httpd_sys_script_exec_t "/var/www/(.*)/cgi-bin(/.+)?"
semanage fcontext -a -t httpd_log_t "/var/www/(.*)/app-logs(/.*)?"
```

semanage fcontext -a -t httpd_log_t "/var/www/(.*)/web-logs(/.*)?" Wenn Logfiles nach /var/www geschrieben werden.

semanage fcontext -a -t httpd_log_t "/var/log/apache/(,*)?" Wenn das Apache log genutzt werden soll

Die Pfade können hier beliebig angepasst werden, je nachdem was man konfigurieren möchte.

restorecon -R /var/www

Datenbankverbindung
setsebool -P httpd_can_network_connect_db on

SOAP Requests an andere Systeme
setsebool -P httpd_can_network_connect on

Mail Versand
setsebool -P httpd_can_sendmail on

User Authentication
setsebool -P httpd_can_connect_ldap on

SSHFS
setsebool -P httpd_use_fusefs on

Filer share
setsebool -P httpd_use_cifs on

Damit werden die Dienste "enabled" die für den Netzwerkbetrieb benötigt werden.

Viel Spass beim Ausprobieren.

Euer Admin