Apache absichern

== Konfigurationsdatei ==
/etc/apache2/apache2.conf

== Weniger Informationen preisgeben ==
Keine Software ist perfekt und selbst nach Bekanntwerden von Sicherheitslücken kann es Tage vergehen, bis das Problem gelöst wird. Daher sollte man sich nicht damit ausweisen welche Software man in welchen Versionen installiert hat.
Eine kurze Google Suche nach Softwareversion und dem Begriff "exploit" und Angreifer erreichen schnell Zugriff.
Um Apache etwas stiller zu machen nehmt ihr folgende Einstellungen vor:

Quellcode

```
1. ServerSignature Off
2. ServerTokens Prod
```

== Zugriff auf fremde Dateien unterbinden ==
Der Apache wird normalerweise so konfiguriert, dass er unter einem eigenen Benutzer läuft. Damit hat er keine Zugriffsrechte auf kritische Verzeichnisse.
Unter Unix-Systemen gibt es noch die Möglichkeit einen Server zusätzlich mit chroot abzusichern. Dies beschränkt den Apache in seinem Zugriff auf einen Teil des Dateibaums. Dies geschieht dadurch, dass der Document Root des Apache die Wurzel des virtuellen Dateibaums wird.

== SVN Dateien verbieten ==
Viele Firmen nutzen SVN um ihre Dateien auf die Produktivsysteme zu deployen. Damit die brisanten Informationen der versteckten SVN Ordner nicht abrufbar sind, sollte man diese über die Apache Konfiguration global sperren.

Quellcode

```
1. <DirectoryMatch "/\.svn/">
2. Order allow,Deny
3. Deny from all
4. </DirectoryMatch>
```