Immer öfter Hört man von Sicherer Verschlüsselter Datenübertragung über SSL. Doch wie richtet man es ein und wie sicher ist SSL wirklich?

allgemeine Konfiguration

Zunächst sollte man dem Apache2 ein paar grundsätzliche Flausen abgewöhnen. Warum verrät er z.B. bei jeder Anfrage seine Versionsnummer und Patchstand?

Forward Secrecy

Wieder so eine Phrase, bei der kein Mensch weiß, um was es sich handelt aber jeder mitreden will.

Damit man nicht dumm stirbt, gibt es hier die Erklärung.

Umsetzung

Um die Verschlüsselung global zu setzen, muss man in der Datei /etc/apache2/mods-enabled/ssl.conf die folgendenen Zeilen eintragen / Ändern

Vorsicht:

In den <VirtualHost>-Anweisungen wird der Wert noch einmal gesetzt und damit überschrieben. Kommentiert ihn bei jedem vHost aus!!

```
SSLProtocol all -SSLv2
SSLHonorCipherOrder On
SSLCipherSuite EECDH+AES:EDH+AES:-SHA1:EECDH+RC4:EDH+RC4:RC4-
SHA:EECDH+AES256:EDH+AES256:AES256-SHA:!aNULL:!eNULL:!EXP:!LOW:!MD5
```

Nachtrag:

1. Leider Ist in der obigen Regel nicht der „anonyme Diffi-Hellmann Schlüsselaustausch“ inbegriffen. dieser sollte wenn mögliche auch abgeschalten werden. Ein `:!ADH` an die Zeile SSLCipherSuite angehängt und auch dieses Problem ist gelöst
2. RC4-Verschlüsselung gilt nicht mehr als sicher und kann mit `!:RC4` deaktiviert werden
3. Aufgrund von Inkompatibilität habe ich mich dazu entschieden, EDH-3DES und EECDH-3DES zu aktivieren. Die Optimierte CipherSuite ist nun

```
SSLCipherSuite EECDH+AES:EDH+AES:-
SHA1:EECDH+AES256:EDH+AES256:EECDH+3DES:EDH+3DES:AES256-
SHA:!aNULL:!eNULL:!EXP:!LOW:!MD5:!ADH
```

HTTP Strict Transport Security

Quellen

Allgemeine Konfiguration

- https://icertificate.eu/de/hilfe/anleitungen/perfect-forward-secrecy-apache.html
- http://www.petefreitag.com/item/505.cfm
- http://www.techrepublic.com/blog/10-things/10-things-you-should-do-to-secure-apache/477/

SSL

Forward-Secrecy

- http://blog.pregos.info/2013/09/05/howto-apache-ssl-and-perfect-forward-secrecy/
- https://blog.benny-baumann.de/?p=1446

HTTP Strict Transport Security

- http://blog.pregos.info/2014/01/31/hsts-was-es-ist-wie-es-funktioniert-und-wie-man-es-in-apache-einrichtet/

SSL Security test

- https://www.ssllabs.com/ssltest/