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, hier die Erklärung.

Beim Aufruf einer Web-Seite wie https://meine-mail.de erfolgt typischerweise ein Schlüsselaustausch über das asymmetrische Verschlüsselungsverfahren RSA. Dabei läuft grob vereinfacht folgende Kommunikation zwischen dem Server der Bank und dem Browser ab:

1. Browser kontaktiert https://meine-mail.de
2. Server präsentiert einen öffentlichen Schlüssel, dem eine vertrauenswürdige Zertifizierungsstelle attestiert hat, dass er tatsächlich der Firma meine-mail gehört
3. Browser überprüft die Unterschrift der Zertifizierungsstelle und ist danach überzeugt, dass er tatsächlich mit meine-mail.de spricht. Er verschlüsselt seine Nachrichten jetzt mit dem soeben erhaltenen öffentlichen Schlüssel.
4. Server kann die Nachrichten mit dem zugehörigen geheimen Schlüssel entschlüsseln.
5. Browser schlägt supergeheim123 als geheimen Sitzungsschlüssel vor
6. Server bestätigt supergeheim123 als geheimen Sitzungsschlüssel

Den ausführlichen Artikel und die Quelle gibt es hier

```
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
```

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/