Sichere SSL Konfiguration

Mit dem „Mozilla SSL Configuration Generator“ läßt sich aktuell wohl am einfachsten und schnellsten eine sichere Konfiguration für den nginx-Webserver erstellen.

Einfach Webserver, Version von Webserver und OpenSSL setzen und zwischen verschiedenen Cipherprofilen wählen, fertig ist eine Beispielkonfiguration.

Der Eintrag zu TLS im Mozilla Wiki ist auch sehr lesenswert.

> Alternativ habe ich hier noch meine (**veraltete**) Anleitung:

Die folgenden Empfehlungen richten sich nach den Empfehlungen von BetterCrypto.org und ihrem Applied Crypto Hardening PDF mit dem Stand vom 21.04.2016.

Folgendes kann man machen, um die Standard-SSL Konfiguration von nginx sicherer zu gestalten:

- Schwache Cipher und Protokolle abschalten
- Webserver soll die Reihenfolge der Ciphers vorgeben
- SSL-Komprimierung ausschalten
- HSTS aktivieren
- Permanente Umleitung von HTTP nach HTTPS aktivieren

Das folgende gilt für nginx unter Debian. Ich trage dabei nur die beiden Direktiven für SSL-Zertifikatsbundle (ssl_certificate) und SSL-Keyfile (ssl_certificate_key) in den jeweiligen server-Block ein. Die restliche SSL-Konfiguration setze ich global in /etc/nginx/nginx.conf (dort gibts bereits einen Teil „SSL Settings“, das Folgende einfach hinzufügen):

```
ssl_prefer_server_ciphers on;
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
ssl_ciphers
'EDH+CAMELLIA:EDH+aRSA:EECDH+aRSA+AESGCM:EECDH+aRSA+SHA256:EECDH:+CAMELLIA128:+AES128:+SSLv3:!
aNULL:!eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!DSS:!RC4:!SEED:!IDEA:!ECDSA:kEDH:CAMELLIA128-
SHA:AES128-SHA';
ssl_dhparam dhparams.pem;
```

Auf Diffie-Hellman aufsetzende SSH-Cipher benötigen eine entsprechende Parameterdatei (ssl_dhparam). Die Standardgröße beträgt 1024 bit. Die Empfehlung nach der Logjam-Attacke sind mind. 2048 bit, besser 4096 bit. Die Datei wird folgendermaßen erstellt (bei 4096 bit dauerte es ca. 5-15 Minuten):

```
# 4096 bit
openssl dhparam -out dhparams.pem 4096
# 2048 bit
```

```
openssl dhparam -out dhparams.pem 2048
```

Danach muss nginx neu geladen/neu gestartet werden!

Revision #4
Created 2021-05-05 07:09:50 UTC by magenbrot
Updated 2021-12-22 14:19:37 UTC by magenbrot