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 Empfehlungen richten sich nach den Vorgaben 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 Apache 2.4 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 Apache 2.4 unter Debian. Ich trage dabei nur die beiden Direktiven für SSL-Zertifikatsbundle (SSLCertificateFile) und SSL-Keyfile (SSLCertificateKeyFile) direkt in den jeweiligen Vhost ein. Die restliche SSL-Konfiguration setze ich global (nach „`a2enmod ssl`“) in /etc/apache2/mods-enabled/ssl.conf. Vorher die bereits konfigurierten Settings auskommentieren (es sollen keine Direktiven doppelt eingetragen sein) und diesen Teil am Ende der Datei einfügen:

```
SSLProtocol All -SSLv2 -SSLv3
SSLHonorCipherOrder On
SSLCompression off
SSLCipherSuite 'EDH+CAMELLIA:EDH+aRSA:EECDH+aRSA+AESGCM:EECDH+aRSA+SHA256:EECDH:+CAMELLIA128:+AE
```

Danach muss Apache neu geladen/neu gestartet werden!

Revision #3
Created 2021-05-05 07:32:50 UTC by magenbrot
Updated 2021-05-05 07:34:43 UTC by magenbrot