Embyserver mit SSL Zertifikat

Getestet mit Ubuntu 18.04 LTS

Um das System eigene Snakeoil verwenden zu können installiert man Apache nach und konfiguiert diesen als SSLHOST. </code> apt install apache2 apache2-utils -y a2enmod ssl a2ensite default-ssl.conf systemctl reload apache2 </code> Ab diesem Zeitpunkt ist unser Server mittels SSL Verschlüsselung auf dem Standardport 443 erreichbar. Um nun dieses Zertifikat auch in Emby nutzen zu können muss es als PFX exportiert werden.

```
openssl pkcs12 -inkey /etc/ssl/private/ssl-cert-snakeoil.key -in
/etc/ssl/certs/ssl-cert-snakeoil.pem -export -out /etc/ssl/certs/ssl-cert-
snakeoil.pfx
```

Hier kann man ein Passwort festlegen, muss es aber nicht. Nun können wir im Emby Webinterface den Pfad des Zertifikates hinterlegen. Folgende Dinge müssen ausgefült werden:

- Externe Domain (FQDN des Servers)
- Eigener SSL-Zertifikatsordner (hier das PFX direkt angeben)
- Passwort zum Ensperren des Schlüssels (optional)

Klickt man auf „Speichern“ startet der Embyserverdienst neu. Ab nun ist der Server auf dem HTTPSport das im Webinterface angegeben wurde (Default 8920) aufrufbar.

Um das ganze noch ein wenig einfacher zu gestalten kann man sich unter `/var/www/html` eine `index.html` mit einer Weiterleitung anlegen.

```
<html>
        <head>
                <meta http-equiv="refresh" content="0;
URL=https://meinembyserver.name.com:8920">
        </head>
</html>
```

Somit ist der Server weiterhin für z.B. intern auf dem Default Nonsslport erreichbar und beim Aufruf des FQDN wird automatisch auf SSL verwießen. Das Zertifikat ist natürlich für Localhost generiert und somit nicht beglaubigt. Wer das ganze offiziell hand haben möchte, kann sich das ganze mit Let's Encrypt basteln.