StartSSL

Zertifikate erzeugen

Aus Sicherheitsgründen sollte man seinen Privaten Schlüssel auf dem eigenen Server erzeugen. StartSSL bietet an, den privaten Key zu erzeugen, aber wer weiß, wo der Private Schlüssel dann landet und was damit gemacht wird. Denn nur mit dem privaten Schlüssel kann man neue Zertifiakte ausstellen oder fälschen (Man-in-the-Middle Attacke)

Privates Schlüsselpaar erzeugen

```
openssl genrsa -out <websitename>_private.key 4096
```

Um jetzt einen Schlüssel bei StartSSL zu bekommen, muss man ein CSR (Certificate Sign Request) erzeugen.

```
openssl req -new -key <websitename>_private.key -out <websitename>.csr
```

es werden nach und nach Informationen über das Zertifikat angefordert. Wichtig ist hier der Common-Name. Dieser sollte der gleiche sein, wie die URL der Webseite.

Zum Schluss werden weitere Einstellungen abgefragt. Hier sollte man ein Passwort hinterlegen, damit der generierte Schlüssel mit einem Passwort geschützt ist.

Nach fertigstellung muss man den generierten csr-Code bei StartSSL eintragen.

nach ein paar Klicks auf weiter und der Eingabe der Domain und Subdomain erhält man das unterschriebene Zertifikatsfile. Dieses als `websitename_ssl.crt` abspeichern. In diesem Dialog sollte man auch das intermediate und root CA Zertifikat herunterladen.

Zum Schluss muss man noch die private Datei entschlüsseln

```
openssl rsa -in <websitename>_private.key -out
<websitename>_private_decrypted.key
```

Hinweis:

Man sollte alle Zertifikate in ein separates Verzeichnis legen (z.B. `/etc/apache/ssl/`) und die Zugriffsrechet 400 ändern. Es wird hiermit verhindert, dass Nicht-root-User Zertifikate einsehen, stehlen, verändern oder neue erstellen können.

Zertifikate einbinden

```
<VirtualHost *:443>
        ServerAdmin webmaster@<websitename>

        ServerName <websitename>

        UseCanonicalName On
        SSLEngine on

        SSLCertificateKeyFile
/etc/apache2/ssl/<websitename>_private_decrypted.key
        SSLCertificateFile /etc/apache2/ssl/<websitename>_ssl.crt
        SSLCertificateChainFile /etc/apache2/ssl/sub.class1.server.ca.pem
        SSLCACertificateFile /etc/apache2/ssl/ca.pem
        SSLCipherSuite HIGH
        SSLProtocol all -SSLv2
        DocumentRoot /var/www/
        <Directory />
                Options FollowSymLinks
                AllowOverride None
        </Directory>
        <Directory /var/www/>
                Options Indexes FollowSymLinks MultiViews
                AllowOverride All
                Order allow,deny
                allow from all
        </Directory>
        ErrorLog ${APACHE_LOG_DIR}/<websitename>-error.log
        LogLevel warn
        CustomLog ${APACHE_LOG_DIR}/<websitename>-access.log combined
</VirtualHost>
```

Quellen

- https://www.digitalocean.com/community/articles/how-to-set-up-apache-with-a-free-signed-ssl-certificate-on-a-vps
- http://www.debacher.de/wiki/Server-Zertifikate_mit_StartSSL