Absicherung eines Webservers mittels SSL

Erstellen eines Schlüssels und Zertifikat-Request-Datei

Für die Erstellung eines privaten Schlüssels inklusive eines Zertifikat Requests ist OpenSSL das Tool der Wahl.

```
#Erstellen eines privaten Schlüssels myPrivateKey inklusive Zertifikat Request myCertificateRequest:
openssl req \
-new -newkey rsa:4096 -nodes \
-keyout www.meinedomain.at.key -out www.meinedomain.at.csr
# Im Anschluß müssen Kontaktdaten der Organisation angegeben werden. Wichtig ist es unter Common Name (CN) den
externen Hostnamen anzugeben.
```

Der private Schlüssel (.key) darf nicht aus der Hand gegeben und nur am Server verspeichert werden. Idealerweise wird der openssl Command direkt am Server in folgendem Systempfad ausgeführt: /etc/pki/ssl/.

XXXX Weiß nicht ob die auf ihren Server das dort ablegen können, bitte mit Serverjungs pfad abklären

Die Zugriffsrechte auf die Schlüsseldatei sollten eingeschränkt werden sodass nur der apache User darauf zugreifen kann. Diese Datei wird direkt in der Apache Konfiguration als SSLCertificateKeyFile verwendet.

Eine gute Dokumentation zum OpenSSL Commandline Tool: http://www.madboa.com/geek/openssl/

Ausstellung eines Zertifikates durch eine CA

Die Zertifikat-Request-Datei (.csr) muss an einen Zertifikat-Authority übermittelt und die Ausstellung eines Zertifikates beantragt werden.

CA für TSN Domains

Nachfolgende Toplevel-Domains sind im Rahmen des TSN durch die DVT registriert worden.

- tsn.at
- tibs.at
- mei-infoeck.at
- konstirol.at

Zertifikate für Subdomains zu oben angeführten Domains können einfach über nachfolgende URL beantragt werden: https://tcs-portal.aco.net/apply/A191/.

Dabei ist folgendes zu beachten.

- Die CSR Datei muss hochgeladen werden.
- Als Gültigkeitszeitraum für das Zertifkat kann 3 Jahre ausgewählt werden.
- Als Variante des Zertifikates wird Server Zertifikat ausgewählt.
- Beim hochladen wird der CN der CSR Datei geprüft, dabei muss es sich um eine Subdomain der oben angeführten Domains handeln. Ansonsten kommt es zu einem Fehler.
- Im Anschluß bitte beim Servicedesk die Ausstellung des Terena Zertifikates beantragen.

- Sobald man von der CA eine Email über die erfolgreiche Ausstellung des Zertifikates erhält kann das Zertifikat (.cer) heruntergeladen werden.

Die Datei wird direkt am Webserver verspeichert und als SSLCertificateFile in der Apache Konfiguration eingetragen.

Als SSLCACertificateFile in der Apache Konfiguration kann die Datei Terena_SSL_CA.ca verwendet werden.

CA für universitäre bzw. schulische Organisationen

Orgainisationen im universitären oder schulischen Umfeld haben die Möglichkeit über die von der ACOnet zur Verfügung gestellten Terena Certificate Services kostenfreie Zertifikate für ihre Domains zu beziehen. Voraussetzung ist dass die Organisation ACOnet Teilnehmer ist und die Zusatzvereinbarung für die Nutzung der Terena Certificate Services abgeschlossen hat.

Alle notwendigen Informationen über die Terena Certificate Services und den Link für die Ausstellung eines Server Zertifikates findet man unter: http://www.aco.net/tcs.html?&L=1.

Als SSLCACertificateFile in der Apache Konfiguration kann die Datei Terena_SSL_CA.ca verwendet werden.

CA für beliebige Organisationen

Falls der Inhaber der Domain nicht berechtigt ist am ACOnet Teilzunehmen empfehlen wir auf folgender Seite eine CA auszuwählen: http://www.psw.net/ssl-zertifikate.cfm?gclid=CM7l4PPT57wCFWoOwwodclgAAg.

⚠ Wird ein Server/Webseite kompromitiert oder der private Schlüssel kommt in falsche Hände, muss umgehend die CA kontaktiert werden um einen Rückruf des Zerifikats (Certificate Revocation) zu veranlassen.

ⓘ Zertifikate haben immer ein Ablaufdatum, es muss darauf geachtet werden rechtzeitig ein neues Zertifikat zu organisieren und am Server zu hinterlegen. Hierfür kann es hilfreich sein die Zertifikat Request Datei (.CSR) aufzubewahren.

Konfiguration von Apache

Folgende SSL Konfiguration kann als good Practise für ein System mit RHEL 6.x oder Centos 6.x übernommen worden. Dabei ist zu beachten, dass die Konfiguration pro virtuellem Host vorzunehmen ist.

```
<VirtualHost IP_Adresse:80>
        ServerName www.meinedomain.at
        Redirect permanent / https://www.meinedomain.at/
</VirtualHost>

<VirtualHost IP_Adresse:443>
        ServerName www.meinedomain.at

        # Jetzt die SSL Config

        SSLEngine on
        SSLProxyEngine on
        SSLOptions +StdEnvVars
        SSLProtocol all -SSLv2
        SSLHonorCipherOrder on
        SSLCipherSuite ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:ECDH+3DES:DH+3DES:RSA+AES:RSA+3DES:!aNULL:!MD5:!
DSS:RC4-SHA

        # Hier gehört die Root CA und mögliche Intermetiat CAs rein
```

```
        SSLCACertificateFile "/etc/pki/ssl/meine_ca.ca"
        SSLCertificateFile "/etc/pki/ssl/www.meindomain.at.crt"
        SSLCertificateKeyFile "/etc/pki/ssl/www.meindomain.at.key"

        # Optional Wenn die Domain und Subdomains nur via HTTPS erreichbar sein soll
        Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"

.....   hier die restliche Config zu der Seite

</VirtualHost>
```

Offizielle Dokumentation von Apache: http://httpd.apache.org/docs/current/ssl/ssl_howto.html