Bechtle-Zertifikat bei Hetzner installieren

Beschreibt Schrtt für Schritt, wie das Bechtle Zertifikat bei Hetzner installiert wird.

Schritt 1: Grundlage

Die Grundlage für die Installation bilden zwei E-Mails. die einmal im Jahr von Bechtle versendet werden.

Die ein enthält als Anhang eine Zip-Datei mit dem Zertifikat, die andere das Passwort für den privaten Schlüssel, welches auch dazu dient die Zip-Datei zu entpacken.

Hierbei entsteht als Extrakt eine .pfx Datei, die wir im nächsten Schritt weiter verarbeiten.

Schritt 2: Zertifikate extrahieren

Nun müssen der private Schlüssel und die Zertifikats-Kette aus der .pfx Datei extrahiert werden.

Dazu starten wir ein Terminal und geben die folgenden beiden Befehle ein.
Es wird dabei ein Passwort abgefragt.
Dieses Passwort identisch mit demjenigen, welches wir zuvor für das Entpacken der .zip Datei benutzt haben.

- Für den privaten Schlüssel:
  `openssl pkcs12 -in <xxx>.pfx -nocerts -out priv-key.pem -nodes`
- Für die Zertifikats-Kette:
  `openssl pkcs12 -in <xxx>.pfx -nokeys -out certificates.pem`

Die .pfx Datei kann jetzt gelöscht werden.

Schritt 3: Zertifikat bei Hetzner einrichten und freigeben.

1. Anmelden bei Hetzner und die KonsoleH wählen.
2. Das gewünschte Produkt auswählen (dedivirt2627.your-server.de) und dort auf bechtle-events.com klicken.
3. Auf der linken Seite unter "Einstellungen" den "SSL Manager" wählen.
4. Nach unten scrollen und "Neues Zertifikat" auswählen.
5. Ganz rechts "Existierendes Zertifikat" => "Hinzufügen"

Nun öffen wir die Datei, die den privaten Schlüssel enthält (priv-key.pem) mit einem Text-Editor und kopieren den gesamten Inhalt beginnend mit: `-----BEGIN CERTIFICATE-----`
bis einschließlich: `-----END CERTIFICATE-----`
in das Feld: "Privater Schlüssel".

Dann öffnen wird die Datei mit der Zertifikats-Kette (certificates.pem) mit einem Text-Editor.

Hier finden wird das eigentliche Zertifikat für *.bechtle-events.com i.d.R. zu oberst, gefolgt von der gesamten Kette der Zertifizierungsstellen.

Das Zertifikat beginnend mit in etwas folgenden Zeilen.

```
Bag Attributes
    localKeyID: 01 00 00 00
    friendlyName: *.bechtle-events.com
subject=C=DE, ST=Baden-Württemberg, L=Neckarsulm, O=Bechtle AG, CN=*.bechtle-events.com
issuer=C=US, O=DigiCert Inc, CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
-----BEGIN CERTIFICATE-----
```

Hiervon kopieren wird alles, angefangen mit: `-----BEGIN CERTIFICATE-----`
bis zum Ende: `-----END CERTIFICATE-----`
in das Feld "Öffentlicher Schlüssel".

Aus dem Rest der Datei entnehmen wir Schritt für Schritt alle weiteren Inhalte beginnend mit `-----BEGIN CERTIFICATE-----` inklusive `-----END CERTIFICATE-----` und kopieren sie der Reihe nach in das Feld "Zwischenzertifikate".

Nun klicken wir auf "Zertifikat importieren" und es sollte oben am Formular eine grüne Bestätigung erscheinen, die uns mitteilt, dass das Zertifikat erfolgreich importiert wurde.

Wir verlassen nun die Seite und gehen zurück zum SSL Manger.

Hier finden wir alle Domains und rechts daneben das aktuell eingestellte Zertifikate.

Hier suchen wir uns eine Domain, die aktuell keine laufende Online-Registrierung bietet und wählen aus der Liste der Zertifikate das neu hinzugefügte aus (Erkennbar am Ablaufdatum, welches neben der *.bechtle-events.com steht und klicken auf den runden Pfeil neben dem Mülleimer rechts neben der Auswahlbox. Hierdurch wird das Zertifikat aktualisiert.

Jetzt rufen wir die Seite https://ssl-trust.com/SSL-Zertifikate/check auf um die ausgewählte Domain zu prüfen. Ist alles korrekt gelaufen, dann sind alle Zertifikatsangaben grün und wir erkennen am Ablaufdatum des ersten Eintrags, dass wir das richtige Zertifikat ausgewählt haben.

Wenn dem so ist, können wir das Zertifikat für alle weiteren Domains auswählen und durch Klick auf den runden Pfeil aktualisieren.

Das war's.