HSTS-Header (HTTP Strict Transport Security) konfigurieren

HTTP Strict Transport Security (abgekürzt HSTS, definiert in RFC6797) ist ein Sicherheitsfeature einer Webseite, das dem Besucher, bzw. dessen Browser sagt, dass sie nur noch per HTTPS verschlüsselt mit ihm kommunizieren will. Dazu wird ein zusätzlicher HTTP-Header gesetzt, der Angaben zum Zeitraum, Umgang mit Subdomains und der Verwendung der HSTS Preloadliste enthält.

Das Feature funktioniert folgendermaßen: Ein Besucher tippt z.B. www.seite-x.de in seinen Browser ein. Der Webserver leitet ihn auf HTTPS um. In der HTTPS-Verbindung wird ein zusätzlicher HTTP-Header gesendet, der bestimmte Informationen für den Browser enthält. Der Browser merkt sich das für den angegebenen Zeitraum. Bei zukünftigen Besuchen greift der Browser dann sofort auf die HTTPS Seite zu.

Es gibt folgende Keywörter:

- `max-age=63072000;` ? innerhalb dieses Zeitraums wird direkt HTTPS angesteuert (Angabe in Sekunden).
- `includeSubDomains;` ? der Eintrag gilt auch für sämtliche anderen Subdomains (vorsichtig damit, wenn andere Subdomains z.B. nicht per HTTPS funktionieren).
- `preload;` ? Google pflegt eine Liste mit Webseiten, die HSTS aktiviert haben. Diese Liste ist in aktuellen Versionen von Chrome, Firefox, Safari, IE11 und Edge enthalten. Diese Webseiten werden sofort per HTTPS angesurft.

Bei nginx muss dazu folgender Eintrag im HTTPS-Teil der Konfiguration gesetzt werden:

```
add_header Strict-Transport-Security "max-age=63072000; includeSubDomains; preload";
```

Nicht vergessen im Vhost für Port 80 die permanente Umleitung auf HTTPS zu konfigurieren. Wie das für nginx zu machen ist, habe ich hier beschrieben.

Danach muss nginx neu geladen/neu gestartet werden!

Wer die Behandlung von HTTP und HTTPS Traffic bei nginx in einem server-Block zusammenfassen möchte, sollte diesen Eintrag von mir beachten.

Revision #1
Created 2021-05-05 07:00:40 UTC by magenbrot
Updated 2021-05-05 07:01:42 UTC by magenbrot