Betreft: Internetconsultatie "Besluit beveiligde verbinding met overheidswebsites en -webapplicaties"
Datum: 5 september 2019
Van: Erik van Straten

Geachte lezer,

Vooraf: doel en werking van HSTS
Het doel van HSTS is het blokkeren van MitM (Man in the Middle) aanvallen, bijvoorbeeld via onvoldoende beveiligde of publieke Wifi-verbindingen, of via DNS-manipulatie (zoals via een ongeautoriseerde wijziging van de DNS-server instelling in een modem/router).
Werking: als een webbrowser over een (nog geldig) HSTS-record voor een website beschikt:
1. Zal deze alle http links (ook zonder protocolaanduiding) naar die site automatisch omzetten in http**s**;
2. Kan de gebruiker een incorrect (mogelijk vervalst) certificaat voor die site niet accepteren.

Een nadeel van HSTS is dat de bescherming ervan pas werkt ***na*** *het eerste bezoek* aan een goed geconfigureerde website - tenzij de website is opgenomen in een “preload” lijst die door veel webbrowsers wordt ondersteund, maar die lijst is momenteel al 9.2MB groot (Nb. Amsterdam.nl lijkt zich hiervoor te hebben aangemeld, maar komt er nog niet in voor). In dit document ga ik er dan ook van uit dat veel overheidswebsites geen gebruik van die preload-lijst zullen maken.

Doel van dit document
Het doel van dit document is het onder de aandacht brengen van een optimale HSTS-configuratie die MitM-risico’s minimaliseert; op veel (ook overheids-) websites kan dit stukken beter dan nu het geval is.

Probleem: www.site.nl versus site.nl
Nb. Voor de duidelijkheid heeft “www.” steeds de kleur rood en schrijf ik http**s** met een vette **s**.
Omdat websites (Nederlandse in dit voorbeeld) zoals www.site.nl meestal ook via site.nl te benaderen zijn, wordt vaak geadverteerd met “ga voor ... naar site.nl”, maar sowieso tikken veel gebruikers slechts “site.nl” in de URL-balk van hun browser. Daarnaast kunnen websites van derden links naar http://site.nl/ bevatten. HSTS werkt alleen goed als *alle* http-links naar een website (zowel hoofd- als “www.” subdomein) door de browser in http**s**-links worden omgezet; helaas is dit is vaak niet het geval.

Toelichting
Bij het bezoeken van site.nl (effectief http://site.nl/) is het gebruikelijk dat de website een *redirect*-instructie naar de browser stuurt, meestal “ga door naar http**s**://www.site.nl/”. Als dat laatste domein HSTS ondersteunt (de juiste header meestuurt), zal de browser voortaan automatisch naar http**s**://www.site.nl/ gaan indien de gebruiker www.site.nl invoert of op de link http://www.site.nl/ klikt. Het probleem is dat *er nog steeds via http* wordt gecommuniceerd als de gebruiker daarna weer “site.nl” intikt of op een link http://site.nl/ klikt: de verbinding kan op dat moment worden gekaapt!

Oplossing
Als optimale HSTS-bescherming gewenst is, en een website zowel via www.site.nl als via site.nl kan worden bezocht (wat meestal het geval is), moeten beide sites zo worden geconfigureerd dat de bezoekende browser meteen voor *beide* domeinen HSTS-gegevens naar de browser stuurt, ongeacht welke van de twee sites de gebruiker probeert te bezoeken. Dit geldt natuurlijk ook voor de omgekeerde situatie dat site.nl de “algemene” site is, en het bezoeken van www.site.nl ertoe leidt dat je op site.nl uitkomt.

Om de problematiek te verduidelijken volgen hieronder een aantal praktijkvoorbeelden (allen gisteren, 4 september 2019, geverifieerd).

Voorbeeld 1: internetconsultatie.nl
Als ik in de URL-balk van mijn browser internetconsultatie.nl (of http://internetconsultatie.nl/) intik, wordt mijn browser doorgestuurd naar http**s**://www.internetconsultatie.nl/.

Wat gaat hier fout:
1. https://www.internetconsultatie.nl/ stuurt *geheel geen* HSTS-header naar mijn browser;
2. Net als bij Arnhem (zie verderop) leidt het bezoeken van https://internetconsultatie.nl/ tot een certificaatfoutmelding omdat die domeinnaam niet in het door de server verzonden certificaat is opgenomen (d.w.z. de server feitelijk niet goed is geconfigureerd).

Voorbeeld 2: venlo.nl
Als ik venlo.nl in de URL-balk van mijn browser intik, wordt mijn browser doorgestuurd naar https://www.venlo.nl/ en ontvangt mijn browser de volgende header:

```
Strict-Transport-Security: max-age=31536000
```

Risico: de volgende keer dat ik venlo.nl in de URL-balk van mijn browser intik, wordt er nog steeds via http gecommuniceerd en kan de verbinding worden gekaapt.
De oorzaak hiervan is tweeledig:
1. Mijn browser wordt niet gevraagd om *ook* verbinding te maken met https://venlo.nl/ waardoor mijn browser geen HSTS-header van dat hoofddomein ontvangt;
2. Hoewel dat hoofddomein https://venlo.nl/ wel bereikbaar is (met een correct certificaat), stuurt deze op dit moment geen HSTS-header naar mijn browser.

Voorbeeld 3: arnhem.nl
Als ik in de URL-balk van mijn browser arnhem.nl intik, wordt mijn browser doorgestuurd naar https://www.arnhem.nl/ en ontvangt mijn browser de volgende header:

```
Strict-Transport-Security: max-age=16070400; includeSubDomains
```

De (optionele en niet altijd begrepen) directive “includeSubDomains” heeft betrekking op www.arnhem.nl en geldt voor alle *subsites* (zoals test.www.arnhem.nl), maar *niet* voor arnhem.nl. Gevolg: de volgende keer dat ik weer arnhem.nl intik in de URL-balk van mijn browser, wordt er *opnieuw* via http gecommuniceerd en kan mijn verbinding op dat moment worden gekaapt.
Het corrigeren van deze situatie is lastiger dan bij Venlo omdat het bezoeken van https://arnhem.nl/ momenteel tot een certificaatfoutmelding leidt (omdat “arnhem.nl” niet in het certificaat is opgenomen, dat de server -onterecht dus- wel verstuurt voor deze website).

Voorbeeld 4: www.denhaag.nl
Hier gaat bijna alles goed (probleem bij omgekeerde situatie). Als ik in de URL-balk van mijn browser www.denhaag.nl intik (of ergens op een link http://www.denhaag.nl/ klik), wordt mijn browser doorgestuurd naar https://www.denhaag.nl/ en ontvangt mijn browser de volgende header:

```
Strict-Transport-Security: max-age=31536000;includeSubDomains
```

Indien ik binnen 31536000 seconden (365 dagen) www.denhaag.nl intik of op http://www.denhaag.nl/ klik, zet mijn browser dit om maar https://www.denhaag.nl/ (zonder dat er via http wordt gecommuniceerd); prima!
Echter, net als bij Arnhem, heeft de HSTS-directive “includeSubDomains” geen effect op het parent-domein “denhaag.nl”. Gevolg: als ik binnen die 365 dagen denhaag.nl intik of op een link http://denhaag.nl/ klik, wordt er *toch* via http gecommuniceerd. Wel gebeurt dit slechts *éénmalig*, omdat:
a) http://denhaag.nl/ mijn browser *eerst* doorstuurt naar https://denhaag.nl/;
b) https://denhaag.nl/ *dezelfde* HSTS-header verstuurt als https://www.denhaag.nl/;
c) https://denhaag.nl/ mijn browser *daarna* doorstuurt naar https://www.denhaag.nl/.
Met andere woorden: als ik mijn eerste bezoek aan de website van Den Haag begin met denhaag.nl communiceert mijn browser één keer via http, terwijl als ik eerst www.denhaag.nl bezoek en binnen een jaar denhaag.nl, gebeurt dat in het totaal twee keer.

Adviezen in relatie tot HSTS

1. Zorg er in ieder geval voor dat beide sites (zowel www.site.nl als site.nl) het https-protocol ondersteunen met een geldig certificaat. Uit kostenoverwegingen kan men het webservercertificaat aanvragen voor zowel "www.site.nl" als "site.nl" (naast eventueel aanvullende subdomeinen). Indien twee verschillende servers worden gebruikt, en het om beveiligingsredenen ongewenst is dat dezelfde private key op verschillende servers staat, kunnen verschillende certificaten worden ingezet (voor HSTS maakt dat niets uit);
2. Overweeg om elke website op het hoofddomein in te richten (dus "site.nl" in plaats van "www.site.nl") en "www.site.nl" (zowel http als https) te laten redirecten naar "https://site.nl/". Naast dat bijv. Google Chrome "www." tegenwoordig weglaat, vereenvoudigt dit de optimale inrichting van HSTS indien het hoofddomein de HSTS directive "includeSubDomains" gebruikt. Toelichting: als de gebruiker www.site.nl invoert, of op een link http://www.site.nl/ klikt, laat de redirect de browser altijd uitkomen op https://site.nl/, waarna "includeSubDomains" ervoor zal zorgen dat alle http links voortaan automatisch naar https worden omgezet voordat de browser via internet communiceert. Voor een discussie hierover zie [1]. **Let op:** het verplaatsen van een website van "www.site.nl" naar "site.nl" kan nieuwe risico's introduceren die allen moeten worden geïnventariseerd en gemitigeerd (o.a. cookies die onbedoeld naar subdomeinen worden gestuurd), en "includeSubDomains" maakt http-verbindingen natuurlijk onmogelijk naar *alle* eventuele subdomeinen;
3. Indien optie 2 onmogelijk of onwenselijk is, zorg er dan voor dat als een browser een willekeurige pagina op https://www.site.nl/ bezoekt, die browser ook altijd verbinding maakt met https://site.nl/, bijvoorbeeld door favicon.ico (of een transparant 1x1 pixel plaatje) altijd van dat hoofddomein te laten ophalen. Dit kost nauwelijks extra performance omdat de meeste browsers dit na de eerste interactie in hun browser-cache zullen opnemen;
4. Indien de opties 2 en 3 onmogelijk of onwenselijk zijn, kan eventueel voor de "Haagse variant" worden gekozen, zoals weergegeven in voorbeeld 4 hierboven. Deze optie is niet optimaal omdat het voor kan komen dat een bezoeker, binnen de HSTS-geldigheidsperiode, tweemaal via http communiceert;
5. Persoonlijk vind ik de HSTS-geldigheidsperiode van veel websites te kort. Als een gebruiker een website zoals van Arnhem slechts één keer per jaar bezoekt, heeft die persoon niets aan HSTS. Ik pleit dan ook voor een geldigheidsperiode van ten minste 35.000.000 seconden (ca. 405 dagen, ruim 1 jaar dus) zodat bezoekers die een website *ongeveer* één keer per jaar bezoeken, kunnen profiteren van HSTS.

Aanvullende informatie

In [2] vindt u een onderzoek dat ik vorig jaar (onder een alias) uitvoerde waaruit blijkt dat o.a. veel overheidswebsites HSTS niet goed implementeren. In [3] reageer ik op het artikel over de internetconsultatie op security.nl. Ook de USA-overheid waarschuwt voor onvolledige HSTS-implementaties in [4] (zie onder "In addition, in many cases, there may never be a first visit to https://domain.gov").

Tot slot

Ik hoop hiermee een zinvolle bijdrage te hebben geleverd aan deze internetconsultatie en uiteindelijk aan de veiligheid van Internet in Nederland.

Met vriendelijke groet,
Erik van Straten
E-mail: ErikvS2005 bij mijn provider in Nederland (xs4all)
secubeter.nl (hier zit momenteel nog geen bereikbare website achter)

[1] https://www.security.nl/posting/576552/Sites+moeten+_www+schrappen%21
[2] https://www.security.nl/posting/566101/NL%3A+veel+brakke+https+sites
[3] https://www.security.nl/posting/622841/Kabinet+wil+https+en+hsts+voor+alle+overheidssites+verplichten#posting622867
[4] https://https.cio.gov/hsts/