Checklist websitemigratie SSL voor ondernemers

Als je als ondernemer een bestaande website migreert van http naar https, zijn er veel dingen waar je aan moet denken. Gebruik deze checklist om er zeker van te zijn dat je niks vergeet bij de implementatie van een SSL-certificaat.

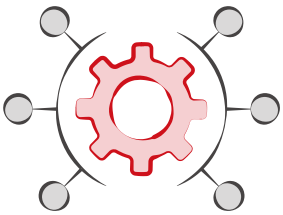
1

Voorbereiding

Webserver en SSL-certificaat

Controleer voor je begint of je webserver geschikt is voor https en laat zo nodig aanpassingen maken door je hostingprovider.

- De webserver moet HTTP Strict Transport Security (HSTS) aankunnen.
- Transport Layer Security (SSL/TLS) moet de nieuwste versie zijn. Op dit moment is dat versie 1.2.
- De server moet Server Name Indication (SNI) ondersteunen, tenzij de server een eigen uniek IP-adres heeft waarop niet meer dan 1 certificaat wordt geïnstalleerd. Overleg dit met de hostingpartij, net als het moment waarop hij het SSL-certificaat moet installeren. Let op, het certificaat moet een 2048-bits sleutel hebben.
- Bespreek met je hostingpartij dat je AES wilt gebruiken als encryptiemethode, en dat de server-CPU ondersteuning biedt voor AES. Dit levert aanzienlijk betere prestaties (snelheid) dan alle andere methodes. Je kunt hierover alles lezen in een diepgravend artikel op de website van MOZ.

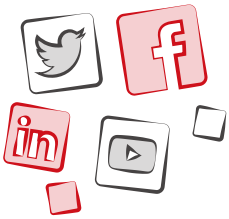


2

CMS en plug-ins

In deze checklist gaan we ervan uit dat je een CMS gebruikt zoals WordPress, Joomla of Drupal, dat geschikt is voor de afhandeling van https-requests. Het is van groot belang dat je controleert of de plug-ins en eventuele custom code waarvan je website gebruik maakt compatible zijn met https. Controleer dit zorgvuldig. Voor elk onderdeel dat niet compatibel is zal je de keus moeten maken:

- De maker om een update vragen;
- De plug-in afschaffen en/of vervangen door een vergelijkbare plug-in.



3

Social shares en likes

Gebruik je een plug-in voor connectie met social media? Dan bestaat de kans dat je likes en shares, kortom de sociale interactie met je gebruikers, niet goed meer worden weergegeven. Dat komt doordat al die interactie wordt gekoppeld aan jouw url's, en die gaan allemaal veranderen. Er zijn verschillende manieren om dat probleem te ondervangen. In dit artikel vind je een uitstekende uitleg.

4

Linkstrategie

We zeiden het al in de inleiding: de overstap naar https is vergelijkbaar met een migratie naar een nieuwe website. Dat komt doordat alle url's, dus al je paginalocaties, veranderen. Er zijn vier soorten links om rekening mee te houden. Relatieve links passen zich automatisch aan naar https als de migratie is voltooid. Deze laten we hier daarom buiten beschouwing.

5

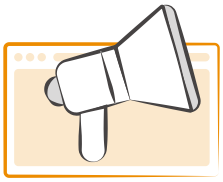
Absolute interne links

Zeer waarschijnlijk zijn niet alle interne links op je site relatief. Handmatig geplaatste links in artikelen bijvoorbeeld, die verwijzen naar andere pagina's op je site. Deze links moet je handmatig aanpassen. Ook links in .css- en .js-bestanden kunnen absoluut zijn. Zorg dat je overzicht van handmatig aan te passen links volledig is.

6

Externe links

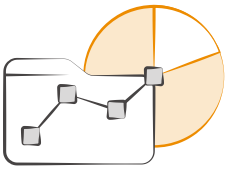
Je hebt zelf geen controle over de links die naar je website verwijzen, maar ze hebben wel veel waarde voor de zoekmachine-ranking. Het is daarom verstandig een lijst te maken van al deze links. Stuur (na de migratie!) een bericht naar de beheerders van elke site met de vraag de links voor je aan te passen. Links die niet worden aangepast leiden we door met redirects (waarover later meer), maar dat kost je wel wat linkjuice.



7

Links in advertenties

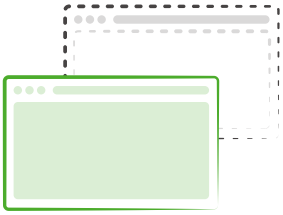
Waarschijnlijk adverteer je op Facebook en Google en mogelijk nog op andere plaatsen. Vergeet dan niet om in al je actieve advertenties de url's om te zetten naar https.



8

Datafeeds

Als je data levert aan derden, zoals vergelijkingssites of Google Shopping, zorg dan dat je datafeeds worden geüpdatet naar de nieuwe https-url's.



9

De migratie

De kern van de migratie behelst niet meer dan het automatisch omzetten van http naar https. Dat doe je met 301-redirects, die de oude url permanent koppelen aan de nieuwe. 301-redirects kun je individueel instellen met een plug-in, maar in dit geval (alle url's moeten immers worden omgezet) doen we het liever op de server.

Op een Apache webserver plaats je daartoe de volgende code in het .htaccess-bestand:

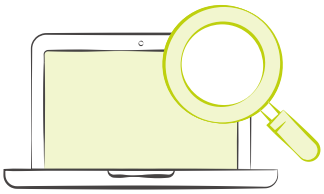
```
RewriteEngine On
RewriteCond %{HTTPS} off
RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI} [R=301,L]
```

Op een Nginx webserver voeg je deze code toe aan het config-bestand:

```
server {
listen 80;
server_name domain.com www.domain.com;
return 301 https://domain.com$request_uri;
}
```

Laat nu je hostingprovider de migratie in gang zetten. Zelf ga je aan de slag met het uitvoeren van je linkstrategie en de volgende stappen:

- ✔ Creëer een nieuwe versie van robots.txt voor https en zet die op je server;
- ✔ Voeg de https-versie van je site toe in Search Console;
- ✔ Check de nieuwe robots.txt in Search Console op fouten;
- ✔ Upload een nieuwe sitemap met alle https-url's;
- ✔ Om de indexering door Google te versnellen kun je losse pagina's of je hele website in Search Console laten ophalen (fetchen als Google).



10

Acceptatietest

Voer een grondige test uit van alle werkzaamheden.

- Controleer of je site geen onveilige content (http) meer bevat. Daarvoor kun je onder meer deze https-linktester gebruiken.
- Check de implementatie van je SSL-certificaat. Het Amerikaanse beveiligingsbedrijf Qualsys heeft daar een handige validatietool voor.
- Test alle sitefunctionaliteiten, zoals de zoekfunctie, filteren, sorteren, gebruikersinteractie, media en abonnementen. Heb je een webshop? Doorloop dan ook een keer het gehele bestel- en betaalproces.

Meer informatie over de veiligheid van je website
Wil je weten of jouw website veilig is? Test het met onze gratis en vrijblijvende webcheck. Met de DTG webcheck krijg je inzicht in de aandachtspunten van je website, het verbeteren van de klantervaring, een concurrentieanalyse & optimalisatietips.