**Artikel 6 |** Het belang van websitebeveiliging met SSL voor SEO

*Steeds meer mensen doen aankopen online. Daarbij delen ze persoonlijke informatie en betaalgegevens. Om te zorgen dat deze gegevens niet in handen vallen van cybercriminelen, is het als ondernemer belangrijk om je website te beveiligen met SSL. En op die manier de privacy en veiligheid van je websitebezoekers te waarborgen. Sinds 2017 neemt Google Chrome de beveiliging van je website mee als SEO-factor. Dat betekent dat Google de websites zonder een SSL-certificaat (ook wel bekend als een TLS-certificaat) beoordeelt als onveilig. In dit artikel lees je wat een SSL-certificaat inhoudt, hoe het werkt en welke invloed het heeft op je positie in de online zoekresultaten.*

**SSL-certificaat**

SSL, dat staat voor Secure Socket Layers, beveiligt de verbinding tussen twee computers. Om te zorgen voor zo’n beveiligde verbinding, is een SSL-certificaat nodig. Dit is in feite een encryptieprotocol dat data en gegevens versleuteld. Het certificaat bevat onder andere gegevens over de houder en uitgever van het certificaat, het domein, de geldigheidsduur en het land waarin het certificaat is uitgegeven. Door je website met een SSL-certificaat te beveiligen, voorkom je dat cybercriminelen de data en gegevens van je bezoekers kunnen achterhalen en misbruiken. Het beveiligen van je website is belangrijk voor iedere ondernemer en organisatie. Voor websites die persoonsgegevens verwerken is een SSL-certificaat zelfs wettelijk verplicht volgens de Algemene verordening gegevensbescherming (AVG). Je bezoekers herkennen een beveiligde website aan het slotje in de adresbalk van de browser en de aanduiding ‘https’ voor de URL. Daarbij staat de afkorting https voor hyper text transfer protocol secure. Met een SSL-certificaat laat je zien dat je de veiligheid en privacy van je bezoekers serieus neemt.

**SSL en SEO**

Sinds 2017 markeert Google Chrome websites zonder SSL-certificaat als onveilig. Een onveilige website herken je aan de rode driehoek met het uitroepteken in de adresbalk van je browser. Bezoekers zien dus direct of ze te maken hebben met een veilige of onveilige website. Door goed beveiligde websites hoger weer te geven in de zoekresultaten, stimuleert Google Chrome het beveiligen van websites en het beschermen van persoonsgegevens. Ben je eigenaar van een website, dan kun je kiezen uit drie verschillende soorten SSL-certificaten:

* Domeinvalidatie: dit type certificaat controleert enkel de domeinnaamhouder op basis van de Whois-gegevens van de domeinnaam. Dit SSL-certificaat is voornamelijk geschikt voor situaties waarbij gegevens veilig verzonden moeten worden, maar waarbij de identiteit van de website zelf minder belangrijk is.
* Organisatievalidatie: dit type certificaat controleert de gegevens van de domeinnaamhouder en de bedrijfsgegevens bij de Kamer van Koophandel. Websitebezoekers kunnen deze gegevens bekijken in het SSL-certificaat.
* Uitgebreide validatie: dit type neemt alle bedrijfsgegevens van de domeinnaamhouder op na een uitgebreide controle bij de Kamer van Koophandel. Ook word je al eigenaar van de website gevalideerd als aanvrager van het certificaat. Bij dit uitgebreide SSL-certificaat, wordt naast het groene slotje ook duidelijk de bedrijfsnaam in de adresbalk getoont.

Het type certificaat dat je kiest, heeft geen invloed op je positie in Google. Wel is het belangrijk om het type certificaat te kiezen dat het beste bij je website past. Een SSL-certificaat is vaak onderdeel van een webhostingpakket. Heb je wel je hosting geregeld, maar beschik je nog niet over een SSL-certificaat? Dan kun je dit certificaat ook los aanschaffen en activeren.

Wil je weten welk SSL-certificaat het beste bij jouw website past of hoe je het certificaat activeert? Bekijk ons aanbod of neem contact met ons op via [contactgegevens].