De veiligheid van onze website

Onlangs bleek dat de allernieuwste versies van Google Chrome, vanaf versie 42, onze website als onvoldoende beveiligd beschouwden, ondanks het feit dat de veiligheid werd gegarandeerd door een certificaat dat door een erkende certificaat autoriteit, Comodo CA, is uitgegeven. Gebruikers van de nieuwste Google Chrome zagen in de adresbalk het volgende:

De reden was dat één van de deelcertificaten was ondertekend met een digitale SHA-1 vingerafdruk, terwijl de SHA-1 hash functie al sinds 2010 als onvoldoende veilig wordt beschouwd. De Calomel SSL validatie, een extensie van Firefox, zag het wat minder somber in en beschouwde onze site nog als zeer veilig, zij het vanwege dat SHA-1 deelcertificaat niet voor 100%, maar voor 88%.

Wij berichtten u daar gisteren over. Sneller dan gedacht kon het certificaat worden vervangen door één waarin SHA-1 niet meer wordt gebruikt. Gebruikers van Google Chrome zien nu weer een groen slotje:

en de Calomel SSL validatie is helemaal tevreden met 100% veiligheid.

Nog wat achtergrondinformatie:

SHA-1 wordt vanwege zijn zwakheden uitgefaseerd, maar daar gaat de nodige tijd overheen omdat veel certificaten langere tijd geldig zijn en er bovendien nog software is die de nieuwere SHA-2 hash functies niet of niet volledig ondersteunt. Daarom beschouwden alle browsers tot voor kort de beveiliging van onze website als voldoende. Al in september vorig jaar maakte Google echter al bekend dat ze binnenkort websites met SHA-1 certificaten die verlopen in 2016 of daarna als onveilig zouden gaan brandmerken. Dat is dus nu, met ingang van versie 42 van Google Chrome, het geval.

U hoefde zich waarschijnlijk niet heel ongerust te maken. Zoals gezegd beschouwde de Calomel SSL validatie onze site nog als zeer veilig, zij het niet voor de volle 100%. Zag Google het te somber in? Misschien, maar ook Microsoft zal na 2016 geen SHA-1 certificaten meer accepteren. Onze website is daar nu op voorbereid.