Onveilige identiteitsbewijzen voor websites moeilijk uit te roeien

21 OKTOBER 2015 09:27 | JELLE WIJKSTRA | NIEUWS 1

20 jaar is in IT-termen een eeuwigheid. We praten over de tijd dat Windows 95 werd gelanceerd. Maar de IT-wereld is nog steeds niet klaar om afscheid te nemen van een beveiligingstechniek voor websites uit die tijd.

Dit jaar worden nog 120.000 certificaten voor websites verstrekt die zijn versleuteld met het algoritme SHA-1, dat in 1995 is ontworpen - 2 jaar nadat het internet voor het algemene publiek toegankelijk werd. 3900 van deze certificaten zijn nog ten minste tot in 2017 geldig. In totaal zijn er nog zo'n miljoen certificaten in omloop die met dit algoritme 'beveiligd' zijn, bleek uit onderzoek van Netcraft waar Paul Mutton enkele details van vrijgaf. Dat aantal komt overeen met een kleine 30 procent van alle certificaten die in omloop zijn.

Al lang als onveilig gezien

Beveiligd stond in de vorige alinea tussen aanhalingstekens omdat SHA-1 al sinds lang niet meer als veilig wordt beschouwd. In 2005 waarschuwde het Amerikaanse National Institute of Standards and Technology al dat SHA-1 onveilig was. 10 jaar later zijn de mathematische zwakheden die SHA-1 vertoont redelijk simpel te exploiteren. Onderzoek van wetenschappers van het CWI, het Franse Inria en de Nanyang Technology University uit Singapore leidt tot de conclusie dat dat met een cluster van 512 GPU's in 49 tot 78 dagen kan. De benodigde rekencapaciteit is in de cloud te huur voor 75.000 tot 120.000 dollar. Dat betekent dat het doenlijk is om cerrtificaten die met SHA-1 zijn ondertekend, te vervalsen. En daarom zijn websites die hun identiteit aantonen met SHA-1-certificaten, feitelijk niet te vertrouwen. Dat geldt bijvoorbeeld voor de Oostenrijke vestiging van Deloitte, die in februari van dit jaar nog een SHA-1-certificaat verkreeg dat geldig is tot 2020, aldus Mutton.

Enkele grote bedrijven niet klaar

Deze situatie is wel eindig. Vanaf 1 januari 2016 mogen geen SHA-1-certifcaten meer uitgegeven worden. Browserleveranciers zijn van plan om vanaf 2017 met SHA-1 ondertekende certificaten te weigeren. Google Chrome waarschuwt al als een certificaat in 2016 verloopt, en noemt websites onveilig als dat certificaat ook na 2016 geldig is. Maar gezien de kostendaling van het kraken van SHA-1 zou deze verouderde technologie beter eerder in de mottenballen kunnen worden gedaan. Dat streven stuit echter op problemen met een aantal grote bedrijven, die zeggen niet sneller te kunnen overstappen op hogere SHA-versies. Symantec diende om die niet ader geïdentificeerde bedrijven terwille te zijn, onlangs het voorstel in om de uitgiftetermijn van SHA-1-certificaten met een jaar te verlengen. Dat voorstel trok het weer in na de jongste schattingen over kosten en duur van een geslaagde SHA-1-kraak

Lees ook

Californië verbiedt encryptie op smartphones 22 JANUARI 2016

Het opvallendste nieuws volgens Hans Timmerman 15 JANUARI 2016

Oud NSA-directeur pleit voor encryptie, net als Cook 14 JANUARI 2016

Wereldwijde oproep voor digitale encryptie 13 JANUARI 2016

OF MEER OVER: SHA, ENCRYPTIE, CERTIFICAAT