© ANP

Nederlandse 'hacker' bewijst: internetbeveiliging verouderd

Het is een Nederlandse onderzoeker gelukt om de beveiliging van het internet, het zogeheten SHA1-systeem, te kraken. Marc Stevens heeft een gat gevonden in de versleuteling die achter de schermen elke e-mail, elke betaling en elk wachtwoord moet beveiligen.

Redactie 23-02-17, 15:37 **Laatste update:** 15:39

Stevens' werkgever, het Centrum Wiskunde & Informatica in Amsterdam, en Google, dat de onderzoeker hielp, hebben de geslaagde aanval vandaag bekendgemaakt. De speciale computers van Google moesten vervolgens 9,2 triljoen (miljard keer miljard) berekeningen uitvoeren, wat een paar maanden kostte. Voor zover bekend is de Nederlander de eerste die met succes door de 'muur' heen komt.

Het SHA1-systeem geeft data een digitale vingerafdruk en die moet volgens Stevens 'uniek en onvoorspelbaar' zijn. ,,Het mag zelfs met inspanning niet lukken om twee berichten dezelfde vingerafdruk te geven''. Dat is de Nederlander nu wel gelukt bij twee pdf-bestanden: ,,Je kunt iemand voor de gek houden, een bestand laten ondertekenen terwijl die dat niet zou willen doen. Je kunt bijvoorbeeld twee facturen maken, de goedkope sturen en laten ondertekenen en dan de dure gebruiken om geld te krijgen. Oplichting dus.''

SHA1 wordt nog veel gebruikt in computersystemen. Stevens roept de tech-wereld op om over te stappen op het nieuwere SHA2-systeem, dat veel sterker en reeds beschikbaar is.

Niet interessant

Voor cyberspionnen is het nu niet interessant om SHA1 te kraken. ,,Een aanval duurt vrij lang en het kost best wat om te ontwikkelen'', legt Stevens uit. ,,Zij hebben andere manieren om hun doelen te bereiken, bijvoorbeeld het besmetten van apparaten en het gebruiken van andere kwetsbaarheden. Dat is gemakkelijker, sneller en toegankelijker.''

,,Ik ben al zeker zeven jaar bezig om tot een zo praktisch mogelijke aanval te komen'', zegt Stevens opgetogen tegenover technologiewebsite Tweakers. ,,Ik denk dat het gelukt is om een methode te ontwikkelen met een zo laag mogelijke complexiteit en door gebruik te maken van zeer geavanceerde cryptanalyse. Het is mooi om dat nu in de praktijk te zien.''