Publicatie : Brabants Dagblad ed. Langstraat
Datum : 15 mrt 2017
Pagina : 24
cm2 : 628
Advertentiewaarde : € 737,00
Regio : Waalwijk
Frequentie : 6x per week
Oplage : 2.857

Waalwijker kraakte samen met Google internetbeveiliging

Een aanval met meer dan 100.000 servers die 9,2 triljoen berekeningen uitvoerden. Spil was Marc Stevens uit Waalwijk, die daarmee een veelgebruikt beveiligingssysteem ontmaskerde.

Jasper Harthoorn
Waalwijk

Even was Marc Stevens uit Waalwijk wereldnieuws. De wetenschapper van het Centrum voor Wiskunde en Informatica (CWI) kraakte samen met collega's en hulp van Google een van de meest gebruikte internetbeveiligingen. Een prestatie die in Nederland weinig opschudding veroorzaakte, maar een kleine aardverschuiving teweegbracht in de technologiewereld. „Een uur nadat we het bekend hadden gemaakt, waren er meer dan 10.000 tweets over verstuurd. Het was meteen trending. Ook de media sprongen erop, vooral de Amerikaanse."
Wat heeft Stevens precies gedaan? Hij beseft dat het voor leken moeilijk uit te leggen is. Hij kraakte het zogeheten *SHA1-systeem*. „Dat is een van de meest gebruikte algoritmes voor digitale vingerafdrukken. Die zorgen er achter de schermen voor dat elke e-mail, website, betaling en elk wachtwoord wordt beveiligd."

Onveilig

Het is Stevens en zijn team gelukt om twee bestanden met dezelfde vingerafdruk te maken. Hiermee kan je een digitale handtekening vervalsen en beveiligingssystemen voor de gek houden. Daarmee toont hij aan dat het beveiligingssysteem dat veel softwarebedrijven als standaard zien, onveilig is. Stevens: „Dat het een kwetsbaar systeem is, was al jaren bekend. Maar nu we het daadwerkelijk gekraakt hebben, móeten softwarebedrijven wel overstappen naar betere beveiligingssystemen. SHA2 en SHA3 zijn wel veilig."
Bij het kraken van een beveiligingssysteem komt veel kijken. Stevens is crypto-analist. Hij kijkt of beveiligingssystemen veilig zijn en of hij wiskundige zwakheden kan aantonen door het systeem te kraken. Bij dit project kreeg hij hulp van Google, dat het ook belangrijk vond aan te tonen dat SHA1 niet langer te vertrouwen is. Het bedrijf stelde zijn processoren ter beschikking. De rekenkracht daarvan is enorm. Via meer dan 100.000 servers over de hele wereld heeft Stevens Google 9,2 triljoen (miljard keer miljard) berekeningen uit laten voeren.
De actie die maanden in beslag nam, klinkt als een utopisch project dat niemand zomaar nadoet. Stevens waarschuwt dat er partijen zijn die dat wél kunnen. Dan denkt hij voornamelijk aan nationale overheden. Hij pakt een verouderd beveiligingssysteem als voorbeeld. Een digitale handtekening van Microsoft, die gebruik maakte van het algoritme MD5, is in het verleden nagemaakt om computers in het Midden-Oosten te bespioneren. Doordat het systeem werd gekraakt, konden hackers windows-updates vervalsen, waardoor machines besmet raakten. De *Washington Post* publiceerde dat Amerika en Israël achter de aanval zaten. Stevens waagt zich er niet aan dat te bevestigen. „Het laat wel zien dat het fout kan gaan. Rusland, China en de Verenigde Staten hebben de middelen én expertise om dergelijke aanvallen uit te voeren."

Ook de media sprongen er meteen op, vooral de Amerikaanse
–Marc Stevens

Voor Stevens lonkt al een nieuwe uitdaging: de quantumcomputer, ofwel supercomputer. „Sommige berekeningen gaan daarmee exponentieel sneller, waardoor de beveiliging van sommige systemen veel makkelijker te kraken is." Voor hem is het zaak dat computersystemen weerbaar zijn als de quantumcomputer in gebruik wordt genomen. Wanneer dat gebeurt, is niet bekend. „We moeten ervan uitgaan dat hij ieder moment kan worden gelanceerd. Dan moeten we er klaar voor zijn."

Publicatie : Brabants Dagblad ed. Langstraat
Datum : 15 mrt 2017
cm2 : 628
Pagina : 24
Advertentiewaarde : € 737,00
Regio : Waalwijk
Frequentie : 6x per week
Oplage : 2.857

▲**Marc Stevens is crypto-analist.**
FOTO JEROEN DE JONG/BEELD

WERKT