Microsoft overweegt SHA-1-certificaten eerder te blokkeren

donderdag 5 november 2015, 10:22 door **Redactie**, 0 **reacties**

Microsoft **overweegt** vanwege recent **onderzoek** om SSL-certificaten met het SHA-1-algoritme een half jaar eerder dan gepland te blokkeren. Uit recentelijk gepubliceerd beveiligingsonderzoek blijkt dat het veel goedkoper is om SHA-1-certificaten aan te vallen dan voorheen werd aangenomen.

Een hashingalgoritme wordt als veilig beschouwd als het voor elke willekeurige invoer een unieke uitvoer heeft en dat die uitvoer niet is terug te draaien zodat de invoer achterhaald kan worden. Doordat de uitvoer niet te manipuleren zou moeten zijn, worden hashes gebruikt om bijvoorbeeld de geldigheid van certificaten en bestanden aan te tonen. Sinds 2005 zijn er echter collision-aanvallen op SHA-1 bekend waar verschillende invoer dezelfde uitvoer geeft.

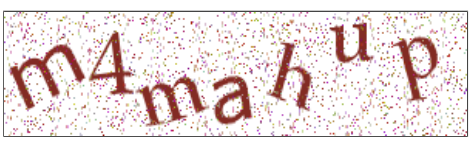
Recent onderzoek van Marc Stevens van het Centrum Wiskunde & Informatica (CWI) uit Amsterdam, Pierre Karpman van het Franse inria en Thomas Peyrin van NTU Singapore laat zien dat het uitvoeren van een dergelijke collision-aanval veel goedkoper kan dan eerst werd aangenomen. Daardoor zouden nu ook criminelen deze aanvallen kunnen uitvoeren. Hierdoor zou het voor kwaadwillenden mogelijk worden om bijvoorbeeld certificaten te vervalsen.

Microsoft had eerder al aangekondigd om SHA-1-certificaten vanaf 2017 te blokkeren, maar overweegt nu om de blokkade volgend jaar juni al in te voeren. Zeven maanden eerder dan gepland. Vorige maand liet **Mozilla** ook al weten dat het overweegt om de SHA-1-blokkade eerder door te voeren, waarbij een datum van 1 juli 2016 werd genoemd. Microsoft zal nu met andere browserontwikkelaars overleggen wat de impact van de voorgestelde nieuwe datum is gebaseerd op gebruik en de haalbaarheid van SHA-1-aanvallen.

Ransomware versleutelt offline computers
Consumentenbond: adblocker bespaart dataverkeer

Ondersteunde bbcodes

Je bent niet ingelogd en reageert "**Anoniem**". Dit betekent dat Security.NL geen accountgegevens (e-mailadres en alias) opslaat voor deze reactie. Je reactie wordt **niet direct geplaatst** maar eerst gemodereerd. Als je nog geen account hebt kun je hier direct een account aanmaken. Wanneer je Anoniem reageert moet je **altijd** een captchacode opgeven.



Herhaal code: