Akkoord

Bijna 1 miljoen websites met 'onveilig' SHA-1-algoritme

maandag 19 oktober 2015, 17:28 door **Redactie**, 5 **reacties**

Onlangs **demonstreerden** onderzoekers dat het veel goedkoper is om SSL-certificaten met het SHA-1-algoritme aan te vallen dan voorheen werd gedacht. Het Centrum Wiskunde & Informatica (CWI) uit Amsterdam pleitte er dan ook voor om het SHA-1-algoritme eerder uit te faseren.

Google Chrome beschouwt SSL-certificaten met het SHA-1-algoritme al als onveilig. Uit onderzoek van internetbedrijf **Netcraft** blijkt echter dat er nog altijd bijna 1 miljoen SSL-certificaten met dit kwetsbare algoritme in gebruik zijn. Het aantal certificaten zal naar verwachting vanaf 2016 afnemen. Het CA/Browser Forum, een consortium van certificaatautoriteiten, de partijen die SSL-certificaten uitgeven, staan dan geen nieuwe certificaten met het SHA-1-algoritme toe.

Hoewel SHA-1 door Google Chrome inmiddels als zwak of onveilig wordt gezien zijn dit jaar nog altijd meer dan 120.000 SHA-1-certificaten uitgegeven. Sommige van deze certificaten zijn tot 2020 geldig, maar zullen eerder moeten worden vervangen. Vanaf 2017 zullen namelijk alle browsers deze certificaten als onveilig weergeven.

Korpschef Politie genomineerd voor Big Brother Award
Firefox 44 laat gebruikers zwakke SSL-websites bezoeken

19-10-2015, 19:08 door Anoniem — Reageer met quote

Waarom gebruikt microsoft dit dan nog voor hun vernieuwde outlook.com?

20-10-2015, 12:34 door Erik van Straten — Reageer met quote

Eerst gokte ik "omdat er nog clients gebruikt worden die geen SHA-2 ondersteunen" maar die lijken sowieso in de kou te staan, want als je https://login.live.com/ (momenteel nog met SHA1 certificaat) opent, wordt CSS en Javascript opgehaald vanaf https://auth.gfx.ms/ welke een SHA-2 (SHA-256 om precies te zijn) certificaat aanbiedt.

Nb. het certificaat van https://login.live.com/ is geldig t/m 30 november aanstaande, en zal dus binnenkort wel worden vervangen.

Overigens is het *intermediate* certificaat voor https://login.live.com/ *ook* met SHA1 is beveiligd, maar ook *dat* is niet het grootste probleem! Het grootste probleem is namelijk dat je er veiligheidshalve vanuit moet gaan dat een aanvaller, gegeven een bestaand certificaat met een geldige digitale handtekening gebruikmakend van SHA1, daar *elk gewenst certificaat* van kan maken.

Om *dat* risico uit te sluiten is het noodzakelijk dat browsers geen enkel SHA1-gebaseerd certificaat meer accepteren.

20-10-2015, 12:57 door Anoniem — Reageer met quote

Bedankt voor je reactie.

Het certificaat van outlook.live.com (het vernieuwe Outlook Mail Preview) is geldig tot 13 februari 2016.
Ik dacht ergens te hebben gelezen dat ze vanaf 1 januari SHA-1 niet meer zouden ondersteunen, maar dat zal dan wel een jaar later zijn.
Mag toch hopen dat ik in het nieuwe jaar nog wel kan inloggen...

20-10-2015, 21:34 door Anoniem — Reageer met quote

@Anoniem 12:57 Vanaf 1 januari 2016 mogen certificaatautoriteiten geen *nieuwe* SHA-1-certificaten meer ondertekenen.

Ja
Nee
Aantal stemmen: **883** 12 reacties

24-01-2016 door Redactie
De directeur van Deutsche Bank heeft deze week tijdens het Wereld Economisch Forum voorspeld dat contant geld binnen 10 jaar ...
Lees meer 43 reacties

20-01-2016 door Arnoud Engelfriet
Een collega van me verloor onlangs zijn tankpas. Hij kreeg keurig een nieuwe, maar in een begeleidende brief (wel apart ...
Lees meer 27 reacties

20-01-2016 door Redactie
Criminelen gebruiken een nieuwe manier om pincodes te stelen die op pinautomaten zijn ingetoetst, namelijk het nemen van ...
Lees meer 56 reacties

16-01-2016 door Redactie
Sinds 1 januari is in Nederland de Meldplicht Datalekken van kracht. Veel bedrijven zitten echter nog met vragen, zo blijkt uit ...

Dit jaar mogen ze dat nog wel doen, mits ondertekende certificaten niet langer geldig zijn dan tot 31 december 2017.

21-10-2015, 09:51 door Anoniem Reageer met quote

@Anoniem 21:34 Bedankt voor de informatie!

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:

Lees meer 16 reacties

09-01-2016 door Redactie

Privacy, en het gebrek eraan, was een onderwerp dat vorig jaar bijna dagelijks in het nieuws kwam en gezien de resultaten van ...

Lees meer 8 reacties

10-01-2016 door Dick99999

Bij de beschrijving van de nieuwe functie 'Emergency access' in LastPass 4.0, staat dat dit ook als backup gebruikt kan worden. ...

Lees meer 3 reacties

07-01-2016 door Heffy

Is er bij de lezers van dit forum enige bekendheid/ervaring met een programma die een lokale back-up maakt van één of ...

Lees meer 14 reacties

© 2001-2016 Security.nl - The Security Council RSS