Moet ik deze week mijn wachtwoorden wijzigen?

By **Marc Hijink**, www.nrc.nl
oktober 24ste, 2017

Herfst. De bladeren vallen, de klok gaat een uur terug en je werkgever vraagt je een nieuw wachtwoord te verzinnen. Alweer drie maanden voorbij. Zo onvermijdelijk als het wisselen van de seizoenen, zo onbegrijpelijk is het dat we braaf een nieuw wachtwoord creëren, telkens als Het Systeem daarom vraagt. Het maakt wachtwoorden tot een nog waardelozer bescherming dan ze al zijn.

Schaf die beperkte houdbaarheid af, adviseert het National Institute of Standards and Technology. NIST stelt richtlijnen op voor Amerikaanse overheidsinstanties en wordt ook serieus genomen door het bedrijfsleven.

Verplicht verversen van wachtwoorden werkt averechts: mensen verzinnen simpele wachtwoorden waar ze telkens maar één teken aan veranderen. Of schrijven hun nieuwe, complexe, wachtwoord op een Post-it-blaadje.

Al in 2009 waarschuwde NIST voor 'wachtwoordvermoeidheid'. We moeten zo veel en zo vaak wachtwoorden verzinnen dat we ze niet meer serieus nemen. Deze zomer, acht jaar later, volgde het officiële advies om het wachtwoordbeleid radicaal te vernieuwen.

Het afschaffen van de houdbaarheidsdatum voor wachtwoorden is voor een systeembeheerder niet meer dan een vinkje zetten in Office 365, de populairste kantoorsoftware. Maar dat is niet voldoende. NIST stelt een tweede verificatiemiddel verplicht, bijvoorbeeld een tijdelijke code van je telefoon, een app of een usb-stick. Verificatie via e-mail is niet veilig, net zo min als vragen naar de naam van je huisdier.

Ook de inhoud verandert. Niet langer hoef je je hoofd te breken op een combinatie van grote en kleine letters, cijfers en symbolen. Wachtwoorden mogen langer zijn, tot wel 64 tekens. Een reeks woorden of een zin is makkelijker te onthouden en moeilijker te kraken.

Het rijtje asterisken ('sterretjes') dat je ziet bij het typen van een wachtwoord, zou niet langer verplicht moeten zijn. Uit angst voor tikfouten verzinnen gebruikers namelijk te eenvoudige wachtwoorden. Een nieuw wachtwoord mag niet voorkomen op lijsten met gestolen wachtwoorden, of in een gewoon woordenboek staan. Iets simpels als *'Abcd1234!'* kan ook niet meer door de beugel, zegt NIST. Organisaties horen wachtwoorden bovendien goed versleuteld te bewaren, zodat ze in geval van diefstal niet op straat komen te liggen.

Wat kun je als gebruiker doen? Zoals altijd: activeer extra verificatie bij webdiensten; zeker bij Apple, Google, Microsoft en je socialemedia-accounts. Gebruik niet hetzelfde wachtwoord bij verschillende webdiensten, en laat een wachtwoordmanager dat probleem oplossen.

Onze wachtwoordvermoeidheid komt voort uit inlogoverkill. Er is bijna geen site meer waar je zonder account iets kunt kopen, downloaden of bekijken. Als dank voor het inloggen word je beloond met spam. Om daar onderuit te komen kun je tijdelijke mailadressen aanmaken via diensten als Maildrop, Guerillamail of PlusPrivacy. Je werkelijke mailadres houd je voor jezelf, en voor je baas.