Hoe lang bestaan wachtwoorden nog? Dit zijn de nieuwe opties

Ze bestaan al jarenlang, de waarschuwingen om uw wachtwoorden zo sterk mogelijk te maken en regelmatig te wijzigen. Er bestaat op 24 november zelfs een speciale dag voor, de Nationale Verander Je Wachtwoord Dag. Maar misschien is dit binnenkort niet meer nodig. Nadert het wachtwoordentijdperk langzamerhand zijn einde?

Wat is het gevaar van wachtwoorden?

Een e-mailadres of gebruikersnaam plus wachtwoord, het is al jarenlang een vertrouwde combinatie op internet. Maar wat als u uw wachtwoord vergeet of kwijtraakt? Of als internetcriminelen uw wachtwoord achterhalen? Of als ergens een groot datalek ontstaat, met ruim 100.000 wachtwoorden, waaronder die van u? Vooral om die laatste reden zoeken experts al langer naar alternatieven voor het klassieke wachtwoord, om het internet veiliger en betrouwbaarder te maken.

Welke alternatieven zijn er?

Het Nationaal Cyber Security Centrum (Ministerie van Justitie en Veiligheid) heeft er een paar op een rij gezet. De 2 belangrijkste zijn multifactorauthenticatie (MFA) en biometrie. MFA is een inlogmethode die uit meerdere stappen bestaat. Denk aan de extra sms-controles, waar DigiD en Facebook gebruik van maken. Biometrie gaat uit van inloggen met unieke lichaamskenmerken, zoals vingerafdrukken, gezichtsherkenning en irisscans.

Zijn de alternatieven al geïntegreerd?

Zeker, beide inlogmethodes zijn inmiddels op grotere schaal ingeburgerd in het internetgebruik. Maakt uw computer bijvoorbeeld gebruik van het besturingssysteem Windows Hello? Dit systeem van Microsoft biedt u de mogelijkheid om via gezichtsherkenning of vingerafdrukken in te loggen. Microsoft heeft dit in 2015 al geïntroduceerd, om op lange termijn de wachtwoorden te vervangen.

Zijn wachtwoorden nu al verleden tijd?

‘Wachtwoorden zijn geen lang leven meer beschoren’, heeft techjournalist Michaël Aussems, hoofdredacteur van IT Daily, dan ook geconcludeerd in 2019. Binnen 4 jaar hebben ze plaatsgemaakt voor veiliger alternatieven, is de verwachting destijds. Liggen we anno 2022 nog altijd op koers? ‘Die ambitie is er nog steeds en het gaat wel degelijk de goede kant op, al gaat het traag’, reageert Aussems tegenover MAX Vandaag.

Welke voordelen bieden de nieuwe inlogmethodes?

Aussems beaamt dat MFA en biometrie de toekomst zijn. MFA kan nog gekoppeld zijn aan een wachtwoord – zoals bij DigiD het geval is – maar het is veiliger om het wachtwoord los te laten. Bijvoorbeeld: een inlogmethode met een vingerafdruk en een controle via uw eigen telefoon. Dat zijn dan niet 1, maar 2 factoren waar alleen u gebruik van kunt maken. Inmiddels is er overigens een extra inlogmethode in ontwikkeling, het ontgrendelen van uw laptop met een speciale usb-stick. Deze zogeheten digitale sleutel heeft het grote publiek echter nog niet bereikt.

Doen de grote spelers op de markt mee?

Het is dus niet zo dat wachtwoorden van de ene op de andere dag direct overbodig zijn. Maar de grote techbedrijven hebben in de afgelopen jaren wel belangrijke stappen gezet. Microsoft is trendsetter op dit gebied en biedt al inlogmogelijkheden zonder wachtwoord aan, net als Apple en Google. Meta, het moederbedrijf van Facebook, Instagram en WhatsApp, is nog iets minder fanatiek, maar werkt ook aan de vernieuwingen.

Kunt u nu al van uw wachtwoord af?

Ja, dat kan. Dat wachtwoorden nu nog bestaan, komt vooral doordat mensen gewoontedieren zijn. En het kan een moeilijke overstap zijn voor mensen die (nog) niet thuis zijn in de digitale wereld. De grote techbedrijven werken daardoor stapje voor stapje toe naar een wereld zonder wachtwoorden, in plaats van alles in 1 keer om te gooien. Maar: ‘Wie wil, kan vandaag al stappen zetten’, aldus Aussems. Heeft u bijvoorbeeld al een melding van Google of Microsoft voorbij zien komen? Met de uitnodiging om een tweestapsverificatie (vorm van MFA) bij het inloggen te gebruiken? ‘Dat is de 1e stap richting het einde van een wachtwoord.’

Is deze methode ook veiliger?

Het komt weleens in het nieuws voor, datalekken en vele internetgegevens die hierdoor in verkeerde handen vallen. Volgens Aussems is 80 procent van alle internetcriminaliteit terug te voeren op het kraken van wachtwoorden. ‘Dat wil zeggen dat 80 procent van de geregistreerde aanvallen niet kon plaatsvinden als er geen wachtwoord was.

MFA, zelfs met wachtwoord, zou het gros daarvan ook al tegenhouden.’ Deze methode kost u bij elke inlogsessie iets meer tijd, maar het is wel een stuk veiliger dan alleen een wachtwoord. De introductie van MFA is de 1e stap, het verdwijnen van de wachtwoorden lijkt de volgende. Voor extra informatie over accountbeveiliging – en alles wat daarbij komt kijken – kunt u terecht bij SeniorWeb.

Bron: IT Daily, Nationaal Cyber Security Centrum (Ministerie van Justitie en Veiligheid), Microsoft, Yubico, SeniorWeb. Foto: Shutterstock)

Dit artikel is bewerkt tot presentatie voor MCCA

Door Dick Beekman