OUCH! | September 2015

Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers.

OUCH!

IN DEZE EDITIE...



# Twee-Factor Authenticatie

## Overzicht

Het bewijzen dat je bent wie je bent (authenticatie) is een belangrijke stap in de beveiliging van je informatie. Een sterke authenticatie zorgt ervoor dat enkel jij toegang hebt tot jouw informatie zoals jouw e-mail, foto's en bankgegevens. Er zijn drie manieren waarmee je je identiteit kan bevestigen: iets dat je weet, bijvoorbeeld een wachtwoord. Iets dat je hebt, bijvoorbeeld een rijbewijs en iets dat je bent, zoals een vingerafdruk. De meest gebruikte methode is wachtwoorden, iets dat je weet. In deze nieuwsbrief hebben we het over hoe je jezelf kan beveiligen met twee-factor authenticatie, een methode die veel veiliger is dan enkel een wachtwoord en zeer eenvoudig te gebruiken is. Om twee-factor authenticatie beter te begrijpen, dienen we eerst een kijkje te nemen naar wachtwoorden.

### Gast redacteur

Keith Palmgren beschikt over meer dan 30 jaar ervaring in informatiebeveiliging. Hij is een gecertifieerde instructeur bij het SANS Instituut en auteur van SANS SEC301 een 5-daagse cursus over introductie tot informatiebeveiliging. Wanneer Keith niet lesgeeft, focust Keith zich op consultancy en schrijfprojecten. Je kan Keith volgen op Twitter via **@kpalmgren**.

## Wachtwoorden

Wachtwoorden bewijzen jouw identiteit op basis van iets dat je weet. Het gevaar met wachtwoorden is dat ze een single point of failure zijn. Indien iemand jouw wachtwoord kan raden of toegang ertoe heeft, kan hij zich voordoen als jou en toegang verschaffen tot alle informatie die met het wachtwoord beveiligd is. Daarom is het belangrijk om sterke wachtwoorden te gebruiken die moeilijk te raden zijn, een ander wachtwoord te kiezen voor iedere account en om nooit jouw wachtwoord te delen met anderen. Hoewel dit advies nog steeds geldt, zijn wachtwoorden niet langer effectief in deze moderne tijd. Moderne technologie maakt het mogelijk voor cyberaanvallers om wachtwoorden snel en eenvoudig te raden of te kraken. We moeten een beter en sterker alternatief gebruiken voor een sterke authenticatie. Gelukkig is er met twee-factor authenticatie een alternatief beschikbaar.

## Twee-factor authenticatie

Twee-factor authenticatie (ook bekend als authenticatie in twee stappen, of twee-staps-verificatie) is een veiligere oplossing dan enkel een wachtwoord. Om je identiteit te bewijzen wordt er niet één maar twee verschillende methodes gebruikt. Een voorbeeld hiervan is jouw bankpas. Wanneer je geld wil afhalen, gebruik je een vorm van twee-factor

# Twee-Factor Authenticatie

authenticatie. Om geld op te nemen, moet je twee dingen hebben. Jouw bankpas (iets dat je hebt) en jouw pincode (iets dat je weet). Verlies je jouw bankpas dan blijft jouw geld veilig. Iemand die jouw bankpas vindt, kan geen geld opnemen omdat men jouw pincode niet weet (tenzij je de pincode op de pas hebt genoteerd, wat een zeer slecht idee is). Hetzelfde geldt wanneer iemand de pincode weet maar de bankpas niet heeft. Een aanvaller moet beiden hebben om toegang te hebben tot jouw bankrekening. Dit is precies wat twee-factor authenticatie zoveel veiliger maakt, er zijn twee beveiligingslagen.


*Maak zoveel mogelijk gebruik van twee-factor authenticatie, het is een van de sterkste maatregelen die je kan nemen om jouw informatie te beschermen.*

## Twee-factor authenticatie gebruiken

Twee-factor authenticatie is iets dat je apart instelt voor elke account. Gelukkig bieden de meeste online diensten dit aan. Een van de leiders in twee-factor authenticatie is Google. Google accounts zijn een belangrijk doelwit voor cyberaanvallers, omdat ze worden gebruikt door miljoenen mensen over de hele wereld voor de reeks van gratis diensten die Google aanbiedt. Net daarom had Google nood aan een sterke authenticatie en was het één van de eerste organisaties die twee-factor authenticatie voorzag voor zijn online diensten. Indien je begrijpt hoe Google's twee-factor authenticatie werkt, begrijp je ook hoe andere sites als Twitter, Facebook, Apple, Instagram en vele banken, twee-factor authenticatie toepassen.

Eerst dien je twee-factor authenticatie in te schakelen op jouw Google account en jouw mobiele telefoonnummer te registreren. Eens voltooid, werkt twee-facor authenticatie als volgt: je logt in met jouw account met jouw gebruikersnaam en wachtwoord. Dit is de eerste factor, iets dat je weet. Google stuurt je dan een SMS naar jouw mobiele telefoon met een unieke code, een reeks van zes cijfers. Net zoals je wachtwoord, geef je deze zes cijfers in op de website. Dit is de tweede factor. Om succesvol in te loggen op je account, dien je het wachtwoord te weten en moet je jouw mobiele telefoon bij de hand hebben om de unieke code te kunnen ontvangen. Zelfs als iemand jouw wachtwoord weet, kunnen ze niet aan jouw Google account zonder jouw mobiele telefoon. Om te verzekeren dat jouw account echt veilig is, stuurt Google je telkens een nieuwe unieke code telkens wanneer je inlogt.

Google en vele andere sites bieden ook een andere manier voor twee-factor authenticatie. In plaats van een unieke code te ontvangen via SMS, kan je een authenticatie app installeren op jouw smartphone. De app zal telkens een unieke code voor

## Twee-Factor Authenticatie

je genereren als je wil inloggen. Het voordeel hier is dat je niet dient verbonden te zijn met een telefoonnetwerk om jouw code te ontvangen, aangezien de telefoon dit voor jou genereert. Bovendien kan de code niet worden onderschept, gezien de code op de telefoon wordt aangemaakt.

Onthoud dat twee-factor authenticatie niet standaard is ingeschakeld, je dient het zelf in te schakelen. Het lijkt op het eerste zicht veel werk, maar we raden aan om dit overal -waar mogelijk- te gebruiken. Zeker voor belangrijke diensten als e-mail accounts, online bankieren of online opslag van bestanden. Twee-factor authenticatie beveiligt jouw informatie veel beter dan enkel een wachtwoord.

## Meer Weten?

Ga naar http://www.securingthehuman.org om je te abonneren op de maandelijkse OUCH! Security awareness nieuwsbrief, toegang te krijgen tot het OUCH! archief en kom meer te weten over SANS security awareness oplossingen.

## Over Cegeka Groep

Cegeka Groep is een onafhankelijke ICT-dienstverlener opgericht in 1992. Cegeka heeft zijn hoofdkantoor in België en heeft vestigingen in België, Duitsland, Frankrijk, Italië, Nederland, Luxemburg, Oostenrijk, Polen, Roemenië, Tsjechië en Slovakije. Het bedrijf levert diensten aan klanten in heel Europa: enterprise cloud- en securitydiensten, applicatiediensten, agile coaching en outsourcingdiensten. Cegeka stelt 3.200 mensen tewerk en haalde in 2013 een omzet van 330 miljoen euro. Bezoek www.cegeka.com voor meer informatie.

## Bronnen (Engels)

| | |
|---|---|
| Passphrases: | http://www.securingthehuman.org/ouch/2015#april2015 |
| Sites Supporting Two-Step Verification: | https://twofactorauth.org |
| Stop\|Think\|Connect: | http://stopthinkconnect.org/2stepsahead |
| Google Two-Step Verification: | http://www.google.com/landing/2step/ |
| SANS Security Tip of the Day: | http://www.sans.org/tip_of_the_day.php |



Redactie: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Vertaald door: Sven Jacobs, Tom Palmaers