Wachtwoord, 2FA of biometrie?

André Reinink

Hackers zijn er dol op en computergebruikers haten het. Enig idee waar ik het over heb? Wachtwoorden! Heeft het wachtwoord zijn beste tijd gehad? Zijn er alternatieven die veilig zijn en voldoen?

Vroeger (heel, heel lang geleden)

Heel, heel lang geleden gebruikte ik voor online accounts overal hetzelfde, voor mij gemakkelijk te onthouden, maar sterke wachtwoord. Vroeger dacht je daar niet over na. Wie kon jouw combinatie van inlognaam en wachtwoord nu achterhalen?

Het werd allemaal anders toen ik thuis een vaste internetverbinding tot mijn beschikking kreeg van wel 1 Mbps. Op dit moment beschik ik thuis over een van de goedkoopste en langzaamste internetverbindingen op mijn adres: een koperaansluiting van 60 Mbps. De bredere beschikbaarheid en snelheid van internet maakt het hackers steeds vaker gemakkelijk.

Later

Wijsheid komt met de jaren. Iedereen zal de situatie herkennen. Je maakt als internetgebruiker steeds vaker een online account aan. Je vertrouwt erop dat de desbetreffende website haar zaken goed voor elkaar heeft. Apropos, ooit wel eens gecontroleerd bij het aanmaken van een account of je een account ook kon verwijderen?

En steeds weer gebruikte ik hetzelfde, sterke, voor mij gemakkelijk te onthouden wachtwoord. Ik las steeds vaker artikelen over websites die gehackt werden. Over inlognamen en wachtwoorden die werden gestolen. Maar als het voor een website is waarbij privacy geen issue is (denk je), waarom zou ik me dan druk maken? Steeds vaker maakte ik accounts aan en ook steeds vaker las ik over ‘hacks’. Tja, wordt het dan niet tijd voor een wachtwoordmanager?

Een wachtwoordmanager?

Online, offline of gewoon een notitieblokje? Omdat internet sinds het begin van deze eeuw steeds beter en sneller is geworden, lag het voor de hand om eens een test te doen met een online wachtwoordmanager.

Ik koos voor een test met ‘LastPass’. Best wel comfortabel. Inloggen met je ‘Master password’ en alle inloggegevens zijn per muisklik beschikbaar.

Maar, alsof het zo moest zijn: LastPass werd getroffen door een hack. Alle gebruikers moesten hun hoofdwachtwoord per omgaande veranderen. Mijn enthousiasme werd behoorlijk getemperd. Enne ... zegt de naam ‘Heartbleed’ je nog iets?

Ik verwijderde het account bij LastPass en stapte over op een lokale wachtwoordmanager: KeePass. Beschikbaar voor vele soorten devices en besturingssystemen. Zo had ik mijn wachtwoorden met KeePass op mijn pc, tablet en smartphone altijd bij de hand.

2018: I have been powned![1]

In 2018 kreeg ik een telefoontje van de systeembeheerder van CompUsers dat mijn CUmail e-mailadres gehackt was. Mijn eerste reactie was: ‘Onmogelijk’. Uit voorzorg werd mijn account gereset en kreeg ik per telefoon een nieuw wachtwoord. Veel later bleek dat ik ooit bij Tweakers.net hetzelfde wachtwoord had gebruikt. Gewoon vergeten aan te passen na een test. En laat nu net dat account bij Tweakers.net, net als dat van vele Tweakers, gehackt te zijn!
Hackers zijn slim en weten heel snel het gejatte account door beschikbaarheid van snel internet te misbruiken. In no-time werd mijn account gebruikt als spam-adres. Na deze gebeurtenis heb ik al mijn accounts onder de loep genomen. Bijna wekelijks merk ik dat mijn e-mail adres nog steeds in trek is bij spammers. Dankzij de adviezen van de systeembeheerder en enig configureren van mijn kant is het aantal spamberichten nu geminimaliseerd.

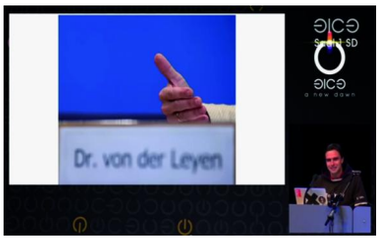
2019: Sterk wachtwoord niet meer afdoende

2019: een sterk wachtwoord is al jarenlang niet afdoende. Ook al heb je een supersterk wachtwoord, je account is kwetsbaar als de site in kwestie haar zaakjes niet goed voor elkaar heeft. Immers: als inloggegevens in een database staan die te hacken is, dan maakt de sterkte van de wachtwoorden niet meer uit. Het moet dus anders en het moet beter.
Een aha-erlebnis was het feit dat mijn ziektekostenverzekeraar aangaf dat ik via DigiD zonder sms-authentificatie niet meer mijn (eigen!) gegevens mocht inzien. De reden hiervoor was dat medische gegevens alleen veilig verstuurd mogen worden. Het moet niet gekker worden. Als alternatief kon ik kiezen voor gegevens per post. Gelukkig is een sms naar een vast telefoonnummer ook mogelijk. Kan dat niet anders?

Is 2FA dan dé oplossing?

2FA staat voor Second Factor Authentification. 2FA is een extra stukje veiligheid bij het inloggen op een computer, server of website. Anders geformuleerd: behalve je inlognaam en wachtwoord is er een aanvullend gegeven nodig: de tweede factor. Dat kan van alles zijn maar die tweede factor is iets wat jij alleen ‘weet’, iets wat alleen jij ‘hebt’ of iets wat alleen jij ‘bent’.
Een voorbeeld van iets wat jij alleen ‘weet’ is het antwoord op een vraag als ‘in welke plaats is je opa geboren’. Je komt dit soort vragen wel eens tegen bij het aanmaken van een account. Een sms’je van jouw verzekeraar is een simpel voorbeeld van ‘iets wat jij alleen hebt’. Immers, via DigiD

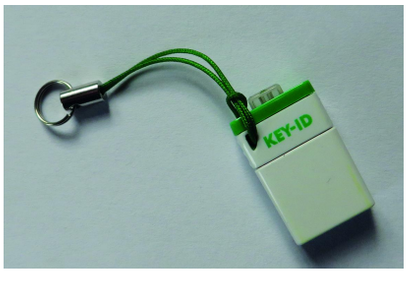
heb je je telefoonnummer gekoppeld. Een hacker is niet in het bezit van jouw telefoon en krijgt dus geen inlogcode via sms. Deze inlogcodes zijn overigens tijdgelimiteerd. Veelal zijn die codes dertig tot zestig seconden geldig. Helaas zijn sms'jes op zich weer niet veilig.



Een voorbeeld van iets wat jij 'bent' zijn bijvoorbeeld vingerafdrukken.
Vingerafdrukken zijn uniek. Ze zijn echter wel na te maken. Actuele discussies: mag je de vingerafdruk van een overledene gebruiken om toegang tot een telefoon te krijgen? Gezichtsherkenning zou ook een voorbeeld kunnen zijn. Besef wel dat een gezicht niet uniek is. Twee nichtjes van mij (een eeneiige tweeling) konden zonder probleem op elkaars iPhone inloggen met behulp van gezichtsherkenning.
Vingerafdrukken, gezichtsherkenning en ook een irisscan zijn zogenaamde biometrische eigenschappen. De Duitse 'Chaos Computer Club' heeft een reputatie hoog te houden als het gaat om het onderuit schoffelen van veiligheid en, in dit geval, inlogmethoden: het met enige moeite deze biometrische eigenschappen namaken.
Voor de gewone man zal men geen moeite doen, wel als je een belangrijk persoon bent natuurlijk. Soms denk ik: hoe simpel kan het zijn? Grote smartphonefabrikanten zetten vingerafdrukken meer en meer aan de kant (de nieuwste iPhone en Google Pixel hebben deze optie niet meer) omdat vingerafdrukken toch niet de ideale beveiliging zijn.

Ik vond het verbazingwekkend dat kort na de introductie van gezichtsherkenning ten gunste van vingerafdrukken bleek, dat ook een gezicht met gesloten ogen geschikt is om in te loggen. Dus, als het slachtoffer ligt te pitten voldoet het om even de smartphone voor zijn of haar gezicht te houden. Dat hadden fabrikanten toch eerder kunnen bedenken? Of denk ik nu te simpel? Gelukkig werd het probleem snel opgelost. 2FA lijkt een betere en veiligere oplossing om in te loggen. Maar de vraag die blijft is: waarmee? En wat dat mag dat kosten?

2FA: Hardware



Geïnspireerd door een artikel van Henk van de Kamer in de PC-Active besloot ik een hardware sleutel, de FIDO U2F USB Security Key[2] te kopen. U2F staat voor Universal 2nd Factor. Dit soort sleutels zijn er in verschillende uitvoeringen en prijsklassen. Ik kocht een relatief universele uitvoering op basis van USB Type A.
De meeste computers hebben wel een USB Type A-poort aan boord. Ook was het zo'n beetje de goedkoopste uitvoering (12 euro). Na ontvangst was het een kwestie van testen. Via deze sites[3,4] zocht ik een proefkonijn uit. Uit de laatste bron koos ik Mail.de[5] en Tutanota[6] uit omdat ze gratis zijn en ze beide een hardwaresleutel (U2F) en een softwaresleutel (TOTP) ondersteunen.
Ik maakte een gratis account aan, al was dat bij de laatste geen eitje. Mocht je een privacy-fetisjist zijn, bekijk dan de Tutanota eens. Tutanota is zelfs zo veilig dat het in verscheidene landen niet toegestaan is. Ik gebruik Tutanota als verdere testcase omdat het Engelstalig is en niet Duits zoals Mail.de en omdat de interface beter geschikt is voor het maken van screenshots voor dit artikel.

Na inloggen ga ik naar de instellingen en vervolgens naar 'second factor authentification'. Ik klik op de '+' om een second factor authentification toe te voegen en kies voor Security Key (U2F).
De verdere procedure is duidelijk en loodst je stap voor stap door de configuratie. Aan het eind van de configuratie krijg je de mogelijkheid een 'recoverycode' te noteren. Mocht je de usb-sleutel kwijtraken of mocht deze defect raken, kun je met deze code de toegang tot jouw account zonder sleutel herstellen. Doen dus.

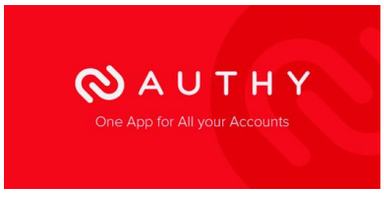
Even testen: na inloggen vraagt Tutanota om de knop in te drukken van de usb-sleutel. Ik druk op de knop en ik ben 'binnen'. Het gebruik van een pas van ziekenhuis- of bankpersoneel is ook een vorm van 2FA. De sleutel is dus een voorbeeld van 'iets wat je hebt'.

Is het gebruik veilig? Ja. Is het handig? Niet altijd. De sleutel die ik gebruik is er ook in andere smaken. Kijk eens op Yubico[7] en ontdek dat ook andere usb-poorten ondersteund worden en zelfs NFC. Maar een feit blijft dat je, om in te loggen met 2FA, je sleutel bij je moet hebben.

2FA: Software

Tutanota ondersteunt ook (T)OTP, Time-based One-Time Password. Ik probeer dit wederom uit bij Tutanota. Nu zou ik dat met de Google Autenticator[8] kunnen doen, maar eigenwijs als ik ben kies ik voor een Open source-oplossing. Henk van de Kamer kiest in zijn artikel voor 'FreeOTP'[9] .

Ik installeer FreeOTP op mijn smartphone met het /e/ besturingssysteem[10]. Ik doorloop dezelfde procedure in Tutanota en kies ervoor om naast de Security-key een 'Authenticator TOTP' toe te voegen. Wel jammer dat FreeOTP alleen een mobiel systeem ondersteunt. Dat moet toch anders kunnen? Ik stuit op een andere oplossing: Authy[11].



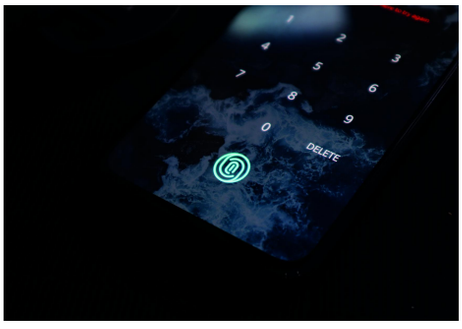
Helaas is Authy, overgenomen door Twilio, geen Open source.
Toch probeer ik Authy uit omdat het:

- meerdere platforms ondersteunt zoals Windows-pc, MacOS, smartphone/tablet en Chrome browser;
- veel sites en accounts ondersteunt;
- back-ups kan maken van de door jou gekoppelde sites en accounts;
- back-ups kan versleutelen;
- mogelijk maakt dat Authy zelf geconfigureerd wordt met een wachtwoord om de software te starten;
- het geen internetverbinding nodig heeft om een geldige sleutel te genereren.

Na een uurtje spelen ben ik 'om' en verwijder ik de FreeOTP-koppeling in Tutanota en maak in plaats daarvan een koppeling met Authy. Ik heb nu een 2FA-mogelijkheid via meerdere devices en platforms.
Met een 2FA heb ik de kans dat ik gehackt wordt wel geminimaliseerd, maar niet onmogelijk gemaakt. Zo zal later blijken.

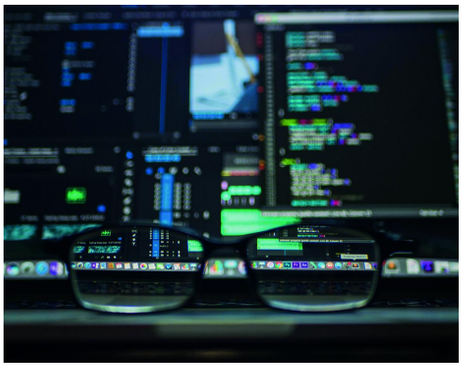
2020: wat staat ons te wachten?

Fabrikanten van smartphones zullen steeds meer, steeds betere en gebruikersvriendelijkere oplossingen gaan bedenken. En omdat een smartphone, simpel gesteld, een doosje propvol sensoren is, ligt het voor de hand dat de smartphone een nog belangrijkere rol in ons, in jouw leven gaat spelen.



Ik durf zelfs te stellen dat jouw smartphone uiteindelijk jouw identiteit gaat worden. Een vingerafdruk alleen is niet veilig genoeg, een simpele gezichtsherkenning is om de tuin te leiden.

Ik vraag me af: 'Waarom hebben Apple en Google niet meerdere technieken gecombineerd?'. De 'big tech five'[12] zijn aan zet. Apple verbetert zijn FaceID iedere keer weer, Google heeft als concurrent 'Soli'[13] geïntegreerd in de Pixel 4. Steeds meer en steeds beter worden biometrische gegevens gecombineerd met steeds meer algoritmes. Ik ga ervan uit dat de lezer de volgende 'mededeling' in dat kader van Google wel begrijpt:



As you reach for Pixel 4, Soli proactively turns on the face unlock sensors, recognizing that you may want to unlock your phone. If the face unlock sensors and algorithms recognize you, the phone will open as you pick it up all in one motion. Better yet, face unlock works in almost any orientation - even if you're holding it upside down - and you can use it for secure payments and app authentification too.[14]

Tjee, die laatste zin schoffelt mijn hele onderzoek naar 2FA en wachtwoorden onderuit. En dit artikel maakt het allemaal ook niet beter[15]. Maar zolang een Pixel 4 of Apple 11 net zoveel kost als een goedkoop, tweedehands autootje en ik nog niet verplicht word te betalen met zo'n device, stel ik dat het artikel de moeite van het onderzoek en het schrijven waard was. En hopelijk het lezen ook:-)

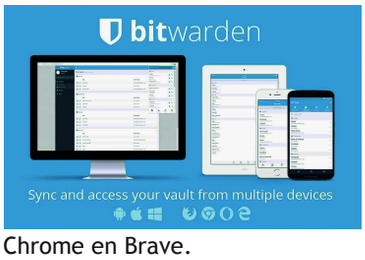
Blijft het bij deze algoritmische 'googlelarij'? Ik denk het niet. Ooit heeft men eens geprobeerd het infrarood aderpatroon van een hand in combinatie met de beweging van de hand als 2FA mee te gebruiken. Zelf gok ik, maar wie ben ik, dat men verder gaat ontwikkelen in een combinatie van een soort biometrische afdruk op een dynamisch gebied op je smartphonescherm (invoer iedere keer op een andere positie) in combinatie met een pincode of gezichtsherkenning.

Zelfs de snelheid, plaats (gps) en tijd waarop je een pincode ingeeft kan een biometrisch gegeven zijn. Uiteindelijk is de volkomen verpersoonlijking van de mens met de smartphone een feit: de 'big tech five' weten alles van jou en alleen met hun algoritmes en technieken kun je ~~betalen~~ leven. Ik ~~betaal~~ leef dus ik besta, zou ik zeggen.

Anno 2020 komt het allemaal steeds sneller dichterbij. Enne, mocht je een flink strafblad hebben, dan vallen een heleboel leuke mogelijkheden met jouw smartphone, die fatsoenlijke mensen wel hebben, natuurlijk af.
Alles is immers van iedereen bekend. Internetcriminelen zijn daarom meer en meer geïnteresseerd in het stelen van andermans identiteit[16].
In 2019 waren er in Nederland meer dan 1,2 miljoen gevallen van identiteitsfraude en -diefstal. George Orwell: waarom heb je daar toentertijd geen oplossing voor bedacht?

Conclusie, Tips & Trucs

Als het mogelijk is, maak dan gebruik van 2FA. Het maakt je nagenoeg ongevoelig voor een hack. Als je 2FA gebruikt zou je kunnen besluiten om simpele, zwakke wachtwoorden te gebruiken. Begrijpelijk maar niet verstandig, het maakt je psychologisch gezien lichtvoetiger op het gebied van internetveiligheid. Maak gebruik van meerdere e-mail accounts. Bijvoorbeeld een account voor privéberichten en een aparte voor internetbestellingen.
CUmail van CompUsers geeft je hiertoe uitgebreide mogelijkheden. Helaas biedt CUmail geen ondersteuning voor 2FA en ook maakt de webmailpagina van CompUsers gebruik van 'Fingerprinting':-(Als je een beperkt aantal sites waar je moet inloggen veelvuldig bezoekt, zou je kunnen overwegen een wachtwoordmanager te gebruiken. Dat kan lokaal met bijvoorbeeld Keepass[17] en in de browser met een add-on of extensie als Bitwarden[18]. De gratis versie van Bitwarden ondersteunt helaas geen 2FA; wel kun je na inloggen gebruik maken van een pincode. Ik heb in KeePass alle wachtwoorden opgeslagen, in Bitwarden enkel een handvol veel gebruikte. Bitwarden is beschikbaar in Firefox, Chrome en Brave.



Onderzoek alles en behoud het goede!

1) https://haveibeenpwned.com/
2) https://www.pcactive.nl/tech/3672-het-lab-freeotp-en-fido-u2f of https://bit.ly/39CC5jj
3) https://www.yubico.com/works-with-yubikey/catalog/ https://bit.ly/2MYj3u0
4) https://www.dongleauth.info/
5) https://mail.de/
6) https://www.tutanota.com/
7) https://www.yubico.com/
8) https://google-authenticator.com/
9) https://freeotp.github.io/
10) https://e.foundation/
11) https://authy.com/
12) https://en.wikipedia.org/wiki/Big_Five_(technology_companies) https://bit.ly/2tBYWuw
13) https://atap.google.com/soli/
14) https://www.aivanet.com/2019/10/does-the-pixel-4-have-a-fingerprint-sensor/ of https://bit.ly/2QqDyBu
15) https://www.zdnet.com/article/chinese-hacker-group-caught-bypassing-2fa/ https://zd.net/37Dqm1X
16) https://www.volkskrant.nl/nieuws-achtergrond/criminelen--hebben-het-steeds-vaker-op-onze-identiteitgemunt~b656b211/ of https://bit.ly/2sOQt7i
17) https://keepass.info/
18) https://bitwarden.com/

Nog meer leesvoer:
https://tweakers.net/reviews/7434/de-toekomst-van-het-wachtwoord-er-moet-iets-veranderen-aan-authenticatie.html https://bit.ly/2QLP8pU
https://www.idin.nl/
https://tweakers.net/reviews/5623/1/biometrie-vloek-of-zegen-inleiding.html https://bit.ly/2QVKeH8
https://www.techzine.be/blogs/security/27728/wat-is-de-toekomst-van-biometrische-authenticatie/
https://bit.ly/2ukSB7f
https://www.europarl.europa.eu/news/en/press-room/20190410IPR37589/improving-data-exchange-between-eu-information-systems https://bit.ly/2QRHJW2
https://www.computable.nl/artikel/opinie/security/6371358/1509029/biometrie-is-mainstream-geworden.html
https://bit.ly/2sELuGt