PATRICK MACKAAIJ

PAS *P JE PASSW*RDS

VANDUUREN MEDIA

Pas op je passwords

Patrick Mackaaij

VANDUUREN
MEDIA

Inhoud

Inleiding

Internet barst van de websites, je smartphone staat vol met apps en steeds meer apparaten zijn verbonden met internet. De combinatie van websites, applicaties en apparaten zal ik in dit boek “diensten” noemen, dat is wat korter.

Voor veel diensten heb je een account nodig. Zo kan de dienst toegang geven tot informatie die op jou van toepassing is. Of onthouden wat je hebt gedaan.

In de meeste gevallen vragen diensten om je e-mailadres. Dat is dan meestal je inlognaam. Om te voorkomen dat andere mensen bij jouw gegevens kunnen, wil een dienst een bewijs hebben dat ze met jou te maken hebben. Hiervoor gebruik je een wachtwoord.

In hun jaarlijkse onderzoek Top 200 Most Common Passwords (2024) [1] hebben de organisaties NordPass en NordStellar een enorme hoeveelheid aan gestolen wachtwoorden onderzocht. Je kunt de top 20 per land bekijken. De conclusie is dat mensen nog steeds zwakke wachtwoorden (her)gebruiken – zowel privé als zakelijk. Als je wachtwoord dan op straat komt te liggen, is het kinderspel voor iemand anders om zich als jou voor te doen. Iemand anders kan een hacker, crimineel of kwaadwillende uit je eigen omgeving zijn.

Door anderen zich als jou voor te laten doen geef je criminelen de kans vrienden en familie te misleiden. En je brengt je werkgever in gevaar – meer dan tachtig procent van de datalekken in bedrijven is terug te voeren naar wachtwoorden van werknemers die zwak of hergebruikt zijn. Bedrijven spelen hier zelf ook een belangrijke rol

in; weinig werknemers krijgen een training cybersecurity op het werk aangeboden.

Bijna de helft van de mensen wijzigt het wachtwoord niet eens als het gehackt is. Sterker nog, mensen geven gewoon hun wachtwoord als je erom vraagt. Bekijk deze twee straatinterviews van Jimmy Kimmel maar eens op YouTube (je kunt de video's vinden door op de titel te zoeken):

- What is Your Password? (2015, **mijn.cc/pw0001**)[1]
- What's Your Password? (2017, **mijn.cc/pw0002**)

Al jaren zijn er geluiden dat wachtwoorden binnenkort verleden tijd zijn. Maar wachtwoorden zijn goed ingeburgerd en blijven echt nog wel even. Je kunt beter orde op zaken stellen en je digitale weerbaarheid vergroten.

De oplossing is al jaren binnen handbereik: het is tijd om een wachtwoordmanager te omarmen. Als je eenmaal een wachtwoordmanager gebruikt is het minder werk én veiliger dan andere werkwijzen om wachtwoorden te onthouden. Inloggen op een wachtwoordmanager is zo gebeurd. Zeker op een smartphone, tablet of moderne computer waar je kunt inloggen met een vingerafdruk of gezichtsherkenning.

Hoeveel accounts heb jij? Ik probeer graag nieuwe dingen uit en zit inmiddels boven de duizend. Mijn wachtwoordmanager onthoudt evenzoveel unieke wachtwoorden. Bijna dagelijks lees ik dat er ergens wachtwoorden zijn gestolen. Regelmatig krijg ik persoonlijk bericht dat er een van mij bij zat. In dat geval verander ik het

1 Door het hele boek zul je de code **mijn.cc/...** tegenkomen; dit zijn verkorte webadressen. Open je browser, typ de complete code in de adresbalk van je browser (in dit gevall **mijn.cc/pw0001**) en je wordt direct naar de juiste pagina op het web geleid!

wachtwoord van die specifieke dienst naar een ander complex wachtwoord, bewaar dat in mijn wachtwoordmanager en ga weer verder met andere bezigheden. Zo eenvoudig kan jij het ook voor jezelf maken.

Dit boek geeft je achtergrondinformatie over het hoe en waarom van een wachtwoordmanager. In het kort:

- Bedenk één wachtwoord of wachtzin. Neem een niet-bestaand woord of zin die nergens voorkomt. Schrijf het eventueel op en berg het thuis goed op als je bang bent dat je het kwijtraakt of beschikbaar wilt hebben voor dierbaren.
- Maak een account aan bij een wachtwoordmanager met dat wachtwoord.
- Installeer de wachtwoordmanager overal waar je deze nodig hebt: op iedere computer, smartphone en tablet en in iedere webbrowser.
- Gebruik de wachtwoordmanager om voor ieder account een uniek, sterk wachtwoord te bedenken en te onthouden. Diensten kunnen onzorgvuldig met je wachtwoord omgaan waardoor het in verkeerde handen terecht kan komen. De schade blijft vanaf nu beperkt tot die ene dienst.
- Als je de mogelijkheid hebt om tweestapsaanmelding in te schakelen, doe het dan. Tweestapsaanmelding ken je vast wel: na het invoeren van je gebruikersnaam en wachtwoord moet je dan nog een code intypen. Gebruik het zeker op je wachtwoordmanager. Gebruik als je kunt kiezen liever codes via een app dan via sms, omdat criminelen je telefoonnummer helaas te eenvoudig kunnen kapen.
- Als je beveiligingsvragen moet beantwoorden, verzin dan een antwoord. Bijvoorbeeld door met je wachtwoordmanager opnieuw een sterk wachtwoord te genereren. Het echte antwoord op een vraag kunnen mensen immers achterhalen of ontfutselen.

- Je hoeft je wachtwoord alleen maar te veranderen als je het vermoeden hebt dat iemand anders je wachtwoord weet. Organisaties die je vragen periodiek je wachtwoord te veranderen, kun je wijzen op de tekst in hoofdstuk 2, in de paragraaf *Verouderd wachtwoordbeleid binnen organisaties*.

Ik heb het boek onderverdeeld in vier delen. In het eerste deel leg ik uit waarom de manier waarop de meeste mensen omgaan met wachtwoorden een probleem is. Vervolgens onderbouw ik in het tweede deel waarom een wachtwoordmanager de beste oplossing is voor het omgaan met wachtwoorden. In het derde deel introduceer ik Bitwarden als wachtwoordmanager. Het vierde en laatste deel laat praktijkvoorbeelden van hacks zien om het belang van een goede omgang met wachtwoorden te onderstrepen.

Ben je al overtuigd dat je een wachtwoordmanager wilt gaan gebruiken? En heb je geen mening over welke dat zou moeten zijn? Dan kun je direct door naar de installatie en het gebruik van Bitwarden. Wil je weten waarom ik voor Bitwarden koos en op basis daarvan je eigen keuze maken, lees dan hoofdstuk 7.

In alle andere gevallen kun je het beste bij het eerste hoofdstuk beginnen.

De kennis in dit boek heb ik niet in mijn eentje vergaard. Mijn kracht is om iets wat stroef loopt op te merken, me erin te verdiepen om vervolgens een betere oplossing te kiezen of te bedenken. Voor het schrijven van dit boek heb ik honderden artikelen op internet gelezen. De beste artikelen van anderen heb ik als voetnoot voor achtergrondinformatie vermeld.

Het idee voor een boek om mensen op weg te helpen met een wachtwoordmanager zat al jaren in mijn hoofd. De online cursus en community Productschool [2] van Erwin Blom gaf mij een vlie-

gende start en stok achter de deur om het boek uiteindelijk te schrijven.

Ingrid Mackaaij, Elisa Huijsman en Sofie Hollak ben ik dankbaar voor de tijd die zij hebben uitgetrokken voor het beantwoorden van mijn vragen over wachtwoorden. Truus Lammerts en Ingrid Mackaaij hebben het boek doorgelezen en gecorrigeerd. Jelte Huisman heeft zijn Android-toestel ter beschikking gesteld voor het nalopen van de instellingen. Ik hoop dat de inhoud van dit boek op basis van hun antwoorden beter is afgestemd op een gemiddelde computergebruiker. Martijn Aslander bracht mij in contact met uitgever Bob van Duuren en Cees Mackaaij heeft de titel bedacht.

En *last but not least* natuurlijk dank aan mijn partner Marjon van Vulpen voor het aanhoren van mijn ideeën en het geven van ruimte naast een druk huishouden met onze twee kinderen.

Deze geactualiseerde tweede druk is te danken aan mijn werkgever Stichting Centraal Register Techniek die gebruikmaakt van de mogelijkheid tot een speciale uitgave met gepersonaliseerde cover als relatiegeschenk. Ik heb Passkeys en Apple Wachtwoorden toegevoegd, Authy vervangen door Ente Auth, YubiKey kanttekeningen gegeven en ten slotte verwijzingen en screenshots geactualiseerd.

Als je een fout in dit boek vindt of als je iets niet begrijpt, dan hoor ik het graag. Ga naar **www.eenmanierom.nl/contact/** en laat een bericht achter. Wil je op de hoogte blijven van nieuwe boeken en artikelen? Schrijf je dan op de website in voor de nieuwsbrief.

Heb je naar aanleiding van dit boek grip gekregen op je wachtwoorden en ben je enthousiast? Dat lees ik graag! Wie weet trek je anderen over de streep om ook hun wachtwoorden op orde te brengen. Je kunt me taggen, meestal kun je me op sociale media vinden als **@mackaaij**.

Meer algemene vragen over wachtwoorden en wachtwoordmanagers kun je – in het Engels of Nederlands – het beste stellen op Quora (**nl.quora.com**). Quora zoekt zelf experts die je vraag kunnen beantwoorden en je kunt mensen specifiek bij een vraag betrekken.

Bronnen

[1] NordPass Top 200 Most Common Passwords: **mijn.cc/pw0001**
[2] Productschool – Maak in 12 weken van je idee een product: **mijn.cc/pw0002**

Deel I
Het probleem

1 Waarom op iedere dienst een ander wachtwoord gebruiken?

Wachtwoorden zouden geheim moeten zijn. En de beste manier om een geheim te bewaren is het aan niemand te vertellen. Helaas werken wachtwoorden anders. Iedere keer als je inlogt moet je je wachtwoord aan een dienst doorgeven. Je moet het letterlijk intypen. Zo is je wachtwoord moeilijk geheim te houden, toch? En welk account denk jij dat belangrijker is? Dat van je e-mail of van je bank?

Verkeerde inschatting van het belang van accounts

Elie Bursztein, een onderzoeker van Google, publiceerde [1] welke accounts het beste beschermd moeten worden:

1 E-mail
2 Sociale media
3 Bank en overige accounts

E-mail staat op de eerste plaats. Via e-mail verstuur je veel persoonlijke informatie. Het belang van een e-mailaccount is de laatste jaren sterk toegenomen, doordat er meer gegevens aan zijn gekoppeld. Denk aan documenten in Google Drive of foto's en documenten bij Apple.

Belangrijker nog: via e-mail kun je bijna al je andere wachtwoorden opnieuw instellen! Als je klikt op **Wachtwoord vergeten** dan krijg je daarvoor vaak een link of code via e-mail.

Sociale media bevatten vaak extra persoonlijke informatie, zoals je geboortedatum, burgerservicenummer, privéberichten en foto's. Ieder stukje extra informatie kan een crimineel gebruiken om zich als jou voor te doen. Soms vergeet je zelfs dat je ergens een account hebt aangemaakt. Helaas gebruiken bedrijven deze relatief eenvoudig te verkrijgen gegevens om bijvoorbeeld tijdens een telefoongesprek te 'bewijzen' dat ze echt met jou te maken hebben. Bedenk maar eens wat de energiemaatschappij, je zorgverlener of je internetprovider ter bevestiging vraagt.

Criminelen kunnen onder jouw account vrienden, familie en collega's overhalen tot het klikken op een link, het overmaken van geld of het afstaan van extra informatie. Ook e-mailberichten aan jou zien er met je naam in de aanhef professioneler uit.

De andere accounts zijn minder belangrijk. Elie Bursztein heeft gevraagd hoe gebruikers daarover denken. De top drie van accounts die het beste beschermd moeten worden is volgens hetzelfde onderzoek:

1 Bank
2 E-mail
3 Sociale media

Dat bankaccounts met stip op nummer één staan is vreemd. Online fraude met je bankaccount kost je maximaal een wettelijk bepaald eigen risico (**en.wikipedia.org/wiki/Bank_fraud**). Dat is veel minder erg dan persoonlijke foto's of teksten die voor altijd op internet vindbaar blijven! Dit is een voorbeeld van het verkeerd inschatten van risico.

Een ander voorbeeld zijn diensten waar je in de loop der tijd meer gebruik van gaat maken, bijvoorbeeld een webwinkel (zoals Amazon of Bol.com). Voor een bestelling geef je al de nodige persoonsgegevens af. Maar op termijn verkoop je misschien zelf (tweedehands) via de etalage van de webwinkel. Wie dan toegang tot je account weet te krijgen, kan het bankrekeningnummer voor de ontvangst van de euro's aanpassen. Of denk aan loyaliteitsprogramma's [2] zoals Air Miles.

Kortom, je schat het belang van accounts verkeerd in én het belang kan geleidelijk aan toenemen. Door voor iedere dienst een ander wachtwoord te gebruiken bescherm je iedere dienst. Als je dat consequent doet hoef je er ook niet meer over na te denken.

Organisaties gaan onzorgvuldig met wachtwoorden om

Bij registreren en inloggen verstuur je je wachtwoord naar een dienst. De communicatie tussen jouw apparaat en de dienst hoort versleuteld te zijn. Helaas is dat nog steeds niet altijd het geval. Als dat niet het geval is, kunnen andere mensen vrij gemakkelijk meelezen. Je herkent een versleutelde verbinding aan het slotje in een webbrowser. Als je een app gebruikt, kun je zelf niet eenvoudig controleren of de verbinding veilig is.

Helpdeskmedewerkers van een dienst kunnen vaak een nieuw wachtwoord voor een gebruiker instellen. RTL Nieuws liet zien dat helpdeskmedewerkers onzorgvuldig omspringen met controleren of zij te maken hebben met de rechtmatige eigenaar van het account [3].

Een dienst hoort vervolgens je wachtwoord zelf niet te bewaren. Criminelen proberen de lijst van alle gebruikers, inclusief persoonsgegevens en wachtwoorden, te kopiëren.

Daarnaast is het de bedoeling dat wachtwoorden ook voor medewerkers van de organisatie geheim blijven. In plaats van je wachtwoord hoort de organisatie een wiskundige verhaspeling van je wachtwoord te bewaren. Verhaspelen is iets anders dan versleutelen. Versleutelen kun je omdraaien – ontsleutelen. Omkeerbaar in wiskunde zijn bijvoorbeeld vermenigvuldigen en delen, optellen en aftrekken of kwadrateren en wortel trekken.

Verhaspelen is onomkeerbaar; het is een zogenoemde *one-way hash*. Een sterk vereenvoudigd voorbeeld van hashen [4] gebruikt een restwaarde. Bijvoorbeeld "de rest bij deling door 5". Als je wachtwoord **6** is, dan is de rest bij deling door 5 de waarde 1. Als je wachtwoord **9** is, dan is de rest bij deling door 5 de waarde 4. De dienst bewaart de waarde 1 of 4 in plaats van het daadwerkelijke wachtwoord. Zelfs als je weet dat de formule "de rest bij deling door 5" is gebruikt, is het onmogelijk om jouw wachtwoord te herleiden.

In dit sterk vereenvoudigde voorbeeld zijn wachtwoorden al snel hetzelfde. De rest bij deling door 5 is bijvoorbeeld 0 bij de wachtwoorden **5**, **10**, **15** enzovoort. In de praktijk zijn veel sterkere hashfuncties in gebruik, met berekeningen die langer duren om criminelen te vertragen.

Helaas is in de praktijk de kans groot dat een dienst je wachtwoord helemaal niet verhaspelt maar gewoon leesbaar (dus zelfs onversleuteld) bewaart. Soms zie je dat zelf doordat je je wachtwoord bij registratie via de e-mail ontvangt. Of een medewerker van de klantenservice leest je wachtwoord van het scherm voor.

In 2019 is onderzoek gedaan door IT-freelancers te vragen de registratie van een sociaal netwerk te verzorgen [5]. Dat zijn de ontwikkelaars die aan de basis van online diensten staan. Veiligheid kreeg pas aandacht als het expliciet onderdeel was van de opdracht.

Technisch ging het dan nog vaak mis doordat wachtwoorden eenvoudig te ontsleutelen waren. Soortgelijk onderzoek was al eerder uitgevoerd met IT-studenten. Zelfs bij grote bedrijven ging het regelmatig mis. Google waarschuwde in 2019 dat het wachtwoorden van zakelijke gebruikers onversleuteld [6] bewaarde.

Er zijn daarnaast mensen die moedwillig websites bouwen om wachtwoorden van de klanten van hun klanten te achterhalen en misbruiken [7].

Het vervoersbedrijf Transport for London (TfL) kwam in 2019 in het nieuws – reizigers moesten hun wachtwoord op een formulier invullen [8].

Bij steeds meer diensten kun je ervoor kiezen om na het inloggen met je inlognaam en wachtwoord een code van zo'n zes cijfers te typen. De basis van deze korte cijfercode is een willekeurig getal. Dat willekeurige getal moeten zowel jouw mobiele telefoon als de dienst bewaren. De technische specificaties [9] adviseren het willekeurige getal versleuteld te bewaren, maar de kans is groot dat dat niet gebeurt.

Opmerking

Business Insider beschrijft hoe Facebook-CEO Mark Zuckerberg met het Facebook-wachtwoord van gebruikers heeft ingelogd op hun e-mail: "In other words, Mark appears to have used private login data from TheFacebook [10] to hack into the separate email accounts of some TheFacebook users." In 2019 had Facebook wachtwoorden onversleuteld opgeslagen [11]. Medewerkers van de klantenservice van Bol.com [12] konden vroeger ook gewoon je wachtwoord lezen.

Kortom, je kunt er niet op vertrouwen dat organisaties zorgvuldig met je wachtwoord omgaan. Door voor iedere dienst een ander wachtwoord te gebruiken, beperk je het risico tot die ene dienst.

Wachtwoorden worden gestolen en gekraakt

Bijna dagelijks zijn er nieuwsberichten over datalekken (*data breaches*) en hacks. Daarbij is dan vaak de lijst van alle gebruikers, inclusief persoonsgegevens en wachtwoorden, buitgemaakt.

In de afgelopen jaren zijn de gebruikerslijsten van grote organisaties zoals Yahoo, Mariott International, Ebay, Quora, LinkedIn, Dropbox en Adobe op straat komen te liggen. Die inloggegevens proberen criminelen vervolgens op andere plekken uit. Bijvoorbeeld voor het plaatsen van bestellingen bij webwinkels [13]. Dit gebeurt ook in Nederland [14].

Daarnaast gebruiken mensen de inloggegevens om je bang te maken en af te persen. Je krijgt dan bijvoorbeeld een e-mailbericht met de mededeling dat je gehackt bent, dat mensen meekijken op je computer en je in de gaten houden via je webcam. Of je even wilt betalen via bitcoin. In het e-mailbericht staat je wachtwoord als ‘bewijs’. Je kunt dergelijke berichten negeren of ze rapporteren bij de fraudehelpdesk [15].

In een nieuwsbericht dat een organisatie zelf over een datalek plaatst staat vaak of de wachtwoorden verhaspeld (gehasht) waren of niet. Verhaspelen van wachtwoorden is onvoldoende. Hackers kunnen aan de hand van woordenboeken, veelgebruikte ‘slimme’ combinaties die mensen toepassen en eerdere wachtwoorden al snel de meeste wachtwoorden achterhalen.

Er zijn zelfs woordenboeken aangelegd om gehashte wachtwoorden te achterhalen. Organisaties die zorgvuldig met je wachtwoord omgaan voegen voor het hashen per gebruiker extra tekens als twist ('zout' of *salt*) toe aan de berekening. Je leest in dat geval over "gesalte gehashte wachtwoorden". Salt vertraagt alleen het kraken van alle wachtwoorden. Als hackers geïnteresseerd zijn in specifieke accounts dan nemen ze het salt gewoon mee in het kraakproces voor specifieke accounts waar zij interesse in hebben.

Opmerking

Voor ontwikkelaars belangrijk om te weten: het leesbaar bewaren van wachtwoorden is strafbaar volgens artikel 32 GDPR/AVG[1]. Hoe moet het dan wel? *Salted Password Hashing – Doing it Right* [16]. Het hashen van alleen het wachtwoord van de gebruiker is onvoldoende. Je moet er per gebruiker (en bij het wijzigen van het wachtwoord) willekeurige tekens (*salt*) aan toevoegen. Salt mag je onversleuteld bewaren. Daarnaast is de aanbeveling los van het gehashte wachtwoord en salt een extra reeks van willekeurige tekens versleuteld te bewaren, bijvoorbeeld in een configuratiebestand (*pepper*).

Kortom, al gaat een organisatie zorgvuldig met je wachtwoord om, het kan op straat komen te liggen. Door voor iedere dienst een ander wachtwoord te gebruiken beperk je het risico tot die ene dienst.

1 General Data Protection Regulation, Algemene verordening gegevensbescherming.

Wachtwoorden delen

In theorie houd je een wachtwoord altijd voor jezelf. Maar soms heb je een generiek account waar een collega ook bij moet kunnen. Of een huisgenoot, denk bijvoorbeeld aan Netflix.

Door voor iedere dienst een ander wachtwoord te gebruiken geef je je collega of huisgenoot eenvoudig gericht toegang tot één account.

Bronnen

[1] Account security – a divided user perception: **mijn.cc/pw0101**

[2] Change Your Loyalty Program Passwords Now: **mijn.cc/pw0102**

[3] RTL Nieuws: Met deze simpele truc zijn 300.000 Tele2-accounts te hacken: **mijn.cc/pw0103**

[4] Cryptographic Hash Functions Explained: A Beginner's Guide: **mijn.cc/pw0104**

[5] 'If you want, I can store the encrypted password.' A Password-Storage Field Study with Freelance Developers: **mijn.cc/pw0105**

[6] Notifying administrators about unhashed password storage: **mijn.cc/pw0106**

[7] Vier jaar voor man die webshops met backdoor ontwikkelde: **mijn.cc/pw0107**

[8] Yes, TfL asked people to write down their Oyster passwords – but don't worry, they didn't inhale: **mijn.cc/pw0108**

[9] TOTP: Time-Based One-Time Password Algorithm > 5. Security Considerations: **mijn.cc/pw0109**

[10] In 2004, Mark Zuckerberg broke into a Facebook user's private email account: **mijn.cc/pw0110**

[11] Keeping Passwords Secure: **mijn.cc/pw0111**
[12] Bol.com medewerker kraakte e-mailaccounts van klanten: **mijn.cc/pw0112**
[13] The Market for Stolen Account Credentials: **mijn.cc/pw0113**
[14] Van Zalando tot Bol.com: duizenden gehackte webshop-accounts doorverkocht: **mijn.cc/pw0114**
[15] Fraudehelpdesk – Hoe herken ik een valse e-mail of een verdacht bericht? **mijn.cc/pw0115**
[16] Salted Password Hashing – Doing it Right: **mijn.cc/pw0116**