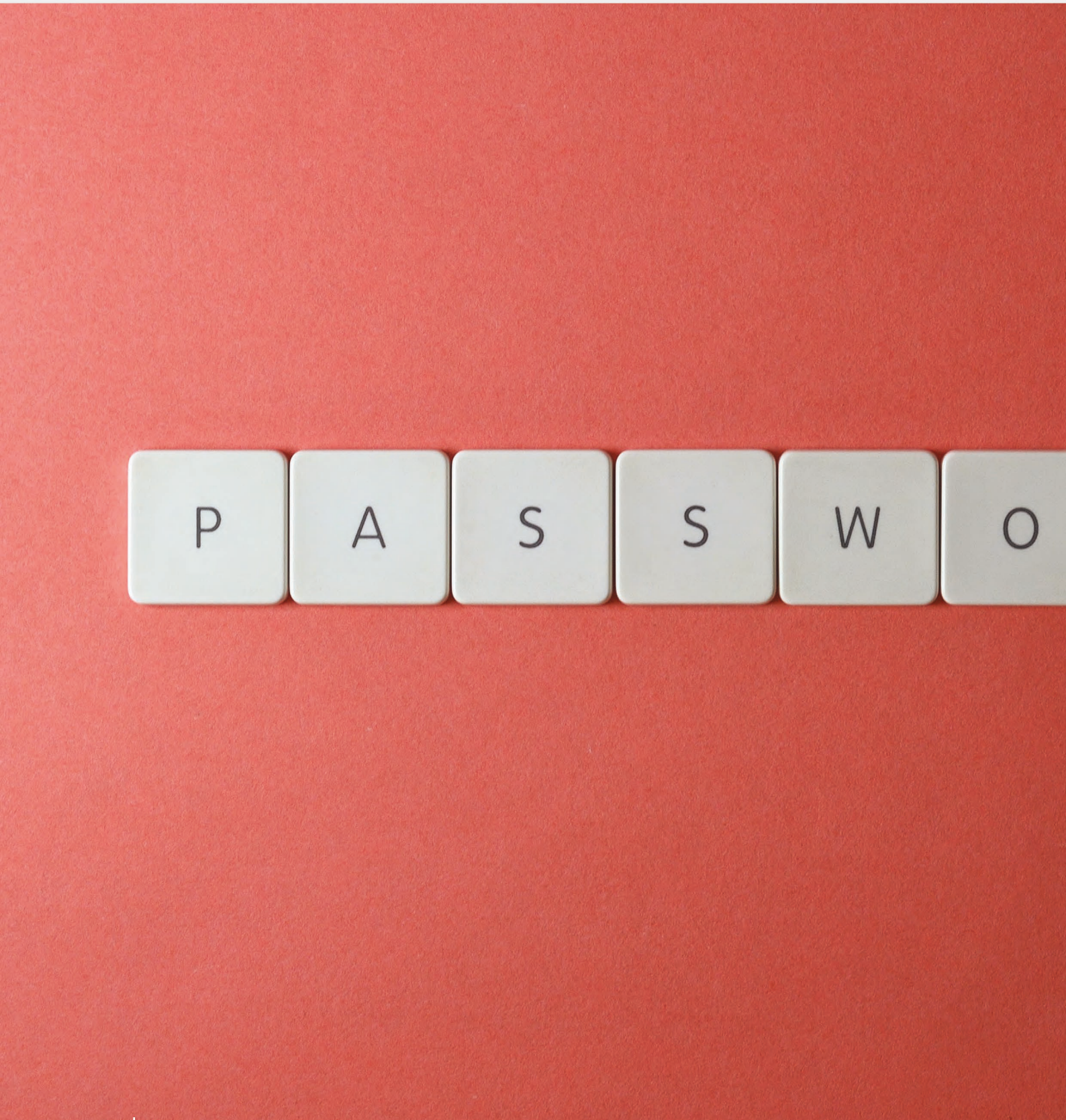
Auteur: Menno Vermeulen is security consultant bij CGI Nederland B.V. Hij is bereikbaar via: menno.vermeulen@cgi.com.



De werking en vele functies van wachtwoordmanagers

Stel je voor dat je in een webshop eindelijk het artikel hebt gevonden dat je wil kopen. Je stopt het in het winkelmandje, maar er komt een ander scherm dat aangeeft dat je eerst een account moet maken. Dit komt vaak voor, omdat er steeds meer online diensten zijn die een account vereisen. Je vult je e-mailadres in en bedenkt een nieuw wachtwoord, waarna je een melding krijgt dat het te kort is én dat je nog een speciaal teken mist. Zonder erbij na te denken voeg je de gevraagde tekens toe en nu heb je een wachtwoord dat je niet meer kunt onthouden

Iedereen weet dat een wachtwoord niet gemakkelijk te raden moet zijn en niet te kort. Veel online diensten helpen je hierbij door bepaalde voorwaarden aan een wachtwoord te stellen, zoals een minimum of een maximum wachtwoordlengte, ten minste één speciaal teken, ten minste één getal, et cetera. Dit verhoogt de *entropie* van het wachtwoord, wat een maatstaf is die beschrijft hoe sterk een wachtwoord is. Een langer wachtwoord met verschillende categorieën van tekens heeft een hogere entropie dan een kort wachtwoord zonder hoofdletters.

Een sterk wachtwoord moet ook uniek zijn en het moet niet worden gebruikt voor verschillende accounts. Als een hacker toegang weet te krijgen tot één account, dan heeft hij ook toegang tot alle andere accounts die hetzelfde wachtwoord gebruiken. Gezien het grote aantal online diensten dat je moet gebruiken, is het echter onmogelijk om al deze wachtwoorden te onthouden. Sommige diensten vereisen zelfs om je wachtwoord periodiek te wijzigen, wat het probleem alleen maar erger maakt.

Een *wachtwoordmanager* lost dit probleem op door al je wachtwoorden in combinatie met je accounts veilig op te slaan. In dit artikel laten we zien hoe wachtwoordmanagers dit doen op het technische vlak. Aan het einde bespreken we veelal aangeboden functionaliteiten van verschillende commerciële wachtwoordmanagers. Zo kun je zelf een goede beslissing maken.

Hoe slaat een wachtwoordmanager alle wachtwoorden op?

Het idee van wachtwoordmanagers is om wachtwoorden op te slaan voor al je accounts, waardoor het heel belangrijk is dat dit veilig gebeurt. Over het algemeen worden de data niet zomaar opgeslagen, maar worden deze eerst versleuteld met behulp van encryptie. *Encryptie* is een proces waarbij data worden gecodeerd naar iets wat geen betekenis meer bezit. Dit met behulp van een *codeersleutel*. Diezelfde codeersleutel kan worden gebruikt om de encryptie om te draaien, waardoor je dus weer de originele data kunt krijgen. Dit heet *decryptie* of *ontsleutelen*.

Het meest gebruikte (symmetrische) encryptie algoritme dat wordt gebruikt in wachtwoordmanagers, is de Advanced Encryption Standard (AES). Dit algoritme voert complexe,

omkeerbare wiskundige bewerkingen uit op blokken data van 128 bits, op basis van de gebruikte codeersleutel. Het resultaat van die bewerkingen is een blok van 128 bits dat versleuteld is, waarvan het origineel alleen maar terug te krijgen is met behulp van de gebruikte codeersleutel. De data, die versleuteld worden, zijn vaak niet precies 128 bits. Als de gegevens meer dan 128 bits zijn, worden ze verdeeld in deze blokken en als er niet genoeg gegevens zijn om een blok te vullen, wordt opvulling gebruikt tot dat wel het geval is.
De codeersleutel die wordt gebruikt in AES kan verschillen in lengte. Volgens de officiële specificatie moet de sleutel 128, 192 of 256 bits zijn (16, 24 of 32 bytes). Hoe langer de codeersleutel, hoe meer moeite het kost om de juiste codeersleutel te raden. Als je de sleutel niet weet, kun je proberen om de versleutelde data te ontsleutelen door iedere mogelijke codeersleutel te proberen. Het zou de beste supercomputer ter wereld al triljoenen jaren kosten om alle mogelijkheden van een codeersleutel van 128 bits te proberen. Door de lengte van de codeersleutel te verhogen, groeit dit aantal exponentieel. Echter, als kwantumcomputers toegankelijker worden, is het mogelijk veel sneller om alle mogelijkheden te proberen. Daarom gebruiken bijna alle wachtwoordmanagers AES-256, met een codeersleutel van 256 bits. De rest van dit artikel gaat uit van een codeersleutel van 256 bits.

Codeersleutel als geheim

Zolang je codeersleutel geheim is, zijn je versleutelde data dat ook. Dit maakt een codeersleutel vergelijkbaar met een wachtwoord en je moet deze dan ook nooit met iemand delen. Er zijn echter cruciale verschillen. Een codeersleutel bestaat uit 256 bits, dat betekent dat iedere bit gebruikt kan worden. Een wachtwoord wordt vaak ingevoerd in een computer. Een computer werkt slechts met bits en bytes, dus ieder teken dat je invoert wordt gecodeerd naar bits.
Een computer kent vaak verschillende coderingen en die moeten ieder teken, inclusief de enter-, backspace- en deletetoets, dat je mogelijk kan invoeren in een computer naar een waarde in bits vertalen. Niet ieder teken kun je gebruiken in een wachtwoord, waardoor er een aantal combinaties van bits zijn die je niet kunt invoeren in een computer. Daardoor is het onmogelijk om met een wachtwoord van 32 tekens iedere mogelijke codeersleutel weer te geven.
In plaats van rechtstreeks een wachtwoord te gebruiken van 32 tekens, wordt een codeersleutel van een wachtwoord afgeleid. Veel wachtwoordmanagers gebruiken hiervoor de 'Password-Based Key Derivation Function 2' (PBKDF2) algoritme. Dit is een 'hash algoritme', dat een algoritme is om met behulp van onomkeerbare wiskundige bewerkingen een unieke code te berekenen voor data. Deze unieke code heet 'hash' of 'hashwaarde', en kan dus niet gebruikt worden om de originele invoer te herleiden. In ons geval is de invoer het wachtwoord dat we hebben en de resulterende hash is de codeersleutel voor onze versleutelde gegevens.
Het PBKDF-algoritme is ontworpen om vele malen herhaald te worden, wat ook wel *iteraties* worden genoemd. Hoe meer iteraties er worden gebruikt, hoe meer moeite een computer moet doen om een hash te berekenen. Als je het wachtwoord weet, hoef je de vele iteraties maar één keer te berekenen, waardoor het alsnog redelijk snel is. Het grote aantal iteraties wordt gedaan om hackers die het wachtwoord willen raden te ontmoedigen, omdat die dan de vele iteraties voor ieder mogelijk wachtwoord moeten berekenen. Het OWASP *Password Storage Cheat Sheet* geeft als advies om PBKDF2 te gebruiken met ten minste 310.000 iteraties.
Om een wachtwoordmanager te gebruiken, heb je een hoofdwachtwoord nodig. Uit dit *hoofdwachtwoord* wordt een codeersleutel afgeleid, die wordt gebruikt om de wachtwoordgegevens te versleutelen voor al je accounts. Omdat dit hoofdwachtwoord **de** sleutel is tot al je accounts, moet het een heel sterk wachtwoord zijn; de entropie moet dus hoog zijn. De meeste wachtwoordmanagers geven ook advies over hoe je een hoofdwachtwoord kunt kiezen.

Bestaande wachtwoordmanagers

Een wachtwoordmanager slaat al je wachtwoorden veilig op. Laten we aannemen dat het bestand met alle inloggegevens voor al je accounts op je computer staat. Om toegang te krijgen tot al je wachtwoorden, moet je het bestand op je computer eerst ontsleutelen. Maar wat als je geen toegang hebt tot die specifieke computer, de computer wordt gestolen of het bestand raakt beschadigd? Dat zou betekenen dat je helemaal geen toegang meer kan krijgen tot al je accounts.
Er zijn veel verschillende wachtwoordmanagers die je kunt gebruiken. Alle wachtwoordmanagers slaan je wachtwoorden veilig op en daarvoor vereisen ze, zoals besproken, een hoofdwachtwoord. De exacte algoritmes die gebruikt worden, kunnen echter verschillen. Daarnaast bieden sommige wachtwoordmanagers extra functies, die worden aangeboden in verschillende soorten abonnementen. Hier bespreken wij een aantal van deze extra functies die bekende wachtwoordmanagers aanbieden, zodat je zelf een weloverwogen beslissing kunt nemen. Er zijn een groot aantal wachtwoordmanagers,

waardoor wij onze beschrijving moeten beperken tot de functies van: LastPass (1), KeePassXC, LessPass, BitWarden, Dashlane en 1Password. Het grote voordeel van het gebruik van een wachtwoordmanager service in vergelijking tot het zelf opslaan, is dat de wachtwoordgegevens worden geback-upt. Met uitzondering van LessPass vereisen alle wachtwoord-managers dat je een account maakt. Voor dit account heb je een hoofdwachtwoord nodig en door daarmee in te loggen heb je toegang tot al je andere wachtwoorden, ongeacht vanaf welk apparaat je inlogt. Als het apparaat waarmee je normaal gesproken je wachtwoorden opzoekt kapot gaat, kun je met een ander apparaat alsnog toegang krijgen tot je wachtwoorden.

Toegangsbeperkingen

De apparaten waarmee je mag inloggen bij je wachtwoord-manager kan afhangen van het abonnement dat je kiest. Met de gratis versie van LastPass kun je bijvoorbeeld ofwel inloggen met je browser vanaf een computer, ofwel inloggen via de app op je mobiel. De betaalde versie heeft deze beperking niet en daarmee kun je dus vanaf ieder apparaat inloggen.
Sommige wachtwoordmanagers bieden ook de optie om een account aan te maken voor meerdere gebruikers. Dit kan aantrekkelijk zijn voor bedrijven, organisaties of grote vrienden-groepen. Eén van de gebruikers moet dan betalen en kan dan anderen uitnodigen. Iedere gebruiker die je toevoegt, kan vervolgens zelf een account aanmaken en gebruikmaken van de functies van de wachtwoordmanager. Als je echter op zoek bent naar een persoonlijke wachtwoordmanager is dit misschien niet de beste optie. Dashlane biedt op dit moment een 'Starter' abonnement aan voor twee dollar per gebruiker per maand, maar je bent verplicht om minimaal tien 'seats', of gebruikers, af te nemen. Hierdoor kost dit abonnement bij Dashlane minimaal twintig doller per maand, omdat je dan ook betaalt voor negen extra gebruikers. Wees op de hoogte van het feit dat dit soort abonnementen bestaan, anders kun je negatief worden verrast.

Wachtwoordgenerators

Bijna alle wachtwoordmanagers hebben een ingebouwde wachtwoordgenerator, die snel willekeurige wachtwoorden genereert op basis van de eisen die je zelf stelt. Zo kun je bepalen uit welke soorten tekens het wachtwoord wordt gegenereerd, of er hoofdletters in kunnen zitten en hoe lang het wachtwoord moet zijn. De gegenereerde wachtwoorden zijn vaak lastig te onthouden, maar ook heel lastig om te raden. Dit is gelukkig geen probleem, omdat de wachtwoordma-nager er juist voor zorgt dat je wachtwoorden niet hoeft te onthouden. De lastig te raden wachtwoorden maken je accounts juist veiliger!

Wachtwoorden delen

Het delen van wachtwoorden is ook een functionaliteit die door veel wachtwoordmanagers wordt aangeboden. Dit lijkt misschien vreemd, omdat een wachtwoord juist geheim moet blijven. Echter, voor sommige onlinediensten kun je een familie-account hebben, of een ander soort account waar misschien verschillende mensen op moeten inloggen. In sommige wacht-woordmanagers kun je je wachtwoord delen door het e-mailadres van iemand in te voeren. Zij krijgen dan een e-mail en als zij inloggen of een account maken bij dezelfde wacht-woordmanager, krijgen zij meteen toegang tot het gedeelde wachtwoord. Als de deler van het wachtwoord het originele wachtwoord verandert, zal deze verandering voor de anderen ook zichtbaar zijn. Er zijn twee verschillende manieren om een wachtwoord te delen. Er is 'one-to-one' delen, waarbij je een wachtwoord kan delen met één ander persoon. Ook is er 'one-to-many' delen, wat het mogelijk maakt om een wachtwoord te delen met een groep personen. LastPass maakt een onder-scheid tussen deze twee manieren en alleen one-to-one delen is beschikbaar voor de gratis versie. Alle andere wachtwoord-managers maken geen onderscheid tussen deze twee typen.

Extra data opslag

Zoals eerder besproken kunnen wachtwoorden opgeslagen worden in een bestand en wachtwoordmanagers kunnen dit op een veilige manier doen. Sommige wachtwoordmanagers gebruiken deze functionaliteit om ook extra bestandopslag aan te bieden. Dit maakt het mogelijk om veilig notities of andere belangrijke documenten op te slaan in je wachtwoord-manager. Doordat de data worden versleuteld, kunnen zelfs hackers zónder jouw hoofdwachtwoord de data niet lezen als het bedrijf achter de wachtwoordmanager wordt gehackt!
Niet alle wachtwoordmanagers bieden deze optie. De wacht-woordmanagers die dat wel doen, bieden verschillende opslagopties, afhankelijk van hoeveel je ervoor wilt betalen. Hoewel dit een leuke toevoeging is aan een wachtwoordma-nager, moet dit niet een reden zijn om een bepaalde wacht-woordmanager te gebruiken. Als de wachtwoordmanager die je wilt gebruiken dit niet heeft, kun je altijd een online dienst vinden die dit wel doet en de accountgegevens in je wacht-woordmanager opslaan.

Waarschuwingen voor inbreuken op de beveiliging

Bijna iedere dag is er een datalek. Het kan zijn dat de website waar jij een account hebt, te maken heeft gehad met zo'n datalek. Sommige wachtwoordmanagers kunnen een notificatie geven als dit het geval is. Soms worden e-mailadressen buitgemaakt, wat ervoor kan zorgen dat je extra spammail krijgt. Cybersecurity-bedrijven houden nauwkeurig in de gaten wat voor datalekken er zijn en wat voor data er op straat liggen. Zodra je wachtwoordmanager ziet dat jouw data daartussen zitten, word je daarop geattendeerd en zul je daar actie op moeten ondernemen. Je zou bijvoorbeeld je wachtwoord moeten veranderen voor dat account.

Multifactor-authenticatie

Het idee van multifactor-authenticatie is dat je meerdere factors gebruikt om je identiteit vast te stellen en om zo in te loggen bij een dienst. Er zijn drie verschillende factoren, die als volgt worden beschreven: 'iets wat de gebruiker weet', 'iets wat de gebruiker heeft' en 'iets wat de gebruiker is'. Een wachtwoord dat je moet invoeren is een typisch voorbeeld van de eerste factor, want dat is iets wat je als gebruiker weet. Een toegangspasje of een authenticator-app op je mobiel is een voorbeeld van de tweede factor. Biometrische gegevens, zoals een vingerafdruk of een gezichtsidentificatie, worden beschreven met 'iets dat de gebruiker is'.

Bij multifactor-authenticatie is het de bedoeling dat je op zijn minst twee factoren gebruikt om je identiteit vast te stellen. Om toegang te krijgen tot je account heb je bijvoorbeeld zowel een wachtwoord nodig als een code die wordt gegenereerd in de authenticator-app op je mobiel. Zelfs als iemand anders dan je wachtwoord weet, heeft diegene alsnog je mobiele telefoon nodig om toegang te krijgen tot je account.

Een wachtwoordmanager is de sleutel tot al je accounts, dus die moet je te allen tijde goed beschermen. Als jouw wachtwoordmanager geen mogelijkheid heeft om multifactor-authenticatie in te stellen, moet je zeker heroverwegen om een andere wachtwoordmanager te nemen.

Automatisch wachtwoorden en gevoelige informatie invullen

Sommige wachtwoordmanagers geven een mogelijkheid om een browser extensie te installeren, waarmee (wachtwoord)velden op websites automatisch kunnen worden ingevuld. Als je je wachtwoord opslaat in een wachtwoordmanager, kun je ook de website waar die op wordt gebruikt toevoegen. Zodra de wachtwoordmanager ziet dat je op die website bent, wordt het wachtwoord automatisch ingevuld, zodat je alleen nog maar op de login-knop hoeft te drukken.

De wachtwoorden die een wachtwoordmanager genereert zijn lastig te onthouden, waardoor dit een uiterst handige functie is. Echter, het makkelijker maken hiervan maakt het minder veilig. Als iemand dan toegang krijgt tot je ontgrendelde computer, worden de wachtwoorden automatisch ingevuld en heeft die persoon dus ook toegang tot al je andere accounts. Multifactor-authenticatie verhelpt dit probleem, omdat er dan nog een extra factor nodig is.

Als je deze functie wel wilt gebruiken, zorg er dan voor dat je je hoofdwachtwoord eigenlijk iedere keer moet invullen voordat de velden worden ingevuld. Dit maakt het misschien iets minder gebruiksvriendelijk, maar het veilig houden van al je accounts gaat niet altijd over gebruiksvriendelijkheid. Een algemeen advies dat altijd geldt: laat je wachtwoord nooit onbeheerd achter!

Ondersteuning

Het is belangrijk om te weten dat je ondersteuning kunt krijgen als je problemen hebt met je wachtwoordmanager. Sommige wachtwoordmanagers zijn 24/7 bereikbaar, andere alleen tijdens kantooruren. Ook kan het afhangen van je abonnement, met een duur abonnement word je vaak eerder geholpen dan wanneer je er gratis gebruik van maakt.

Ondersteuning kan bestaan uit een live-chat, per e-mail, of telefonisch. Niet alle wachtwoordmanagers bieden alle opties en ook dit kan afhankelijk zijn van je abonnement. Als je problemen het liefst wilt oplossen via de telefoon, zorg er dan voor dat je een wachtwoordmanager kiest die die service ook biedt.

Reputatie

Ook de reputatie van een wachtwoordmanager kan bepalend zijn voor je keuze. De reputatie van een wachtwoordmanager wordt ondersteund door de functies die geboden worden, de specifieke algoritmes die worden gebruikt om de wachtwoorden te versleutelen, de technische ondersteuning die geboden wordt, maar ook datalekken die in het verleden zijn gebeurd. Wachtwoordmanagers zijn een belangrijk doelwit voor hackers, omdat ze toegang kunnen krijgen tot iedere account van iedere gebruiker wanneer ze toegang krijgen tot alle gegevens van een wachtwoordmanager.

Een datalek is een serieus probleem, maar soms is het onmogelijk om het te voorkomen. Of een wachtwoordma-

De beste wachtwoordmanager is degene die je gemakkelijk kunt gebruiken en degene die je vertrouwt om jouw accounts veilig te houden.

nager betrouwbaar is of niet hangt ook af van hoe het bedrijf is omgegaan met de datalekken die hebben plaatsgevonden. Wat voor soort gegevens zijn er gestolen? Heeft het bedrijf de inbreuk op een verantwoorde manier afgehandeld? Een bedrijf dat een datalek verantwoord heeft afgehandeld, is misschien betrouwbaarder dan een bedrijf waar nog nooit een datalek heeft plaatsgevonden.
Denk eraan dat de reputatie van een wachtwoordmanager een belangrijke factor is, maar niet de enige factor. Het is ook belangrijk om de functies en beveiliging van een wachtwoordmanager zorgvuldig te evalueren om er zeker van te zijn dat deze voldoet aan je eigen behoeften en dat deze het beschermingsniveau biedt dat je zelf nodig hebt.

'Stateless' wachtwoordmanager

LessPass is een heel ander type wachtwoordmanager, want deze is 'stateless'. Dit betekent dat de wachtwoordmanager helemaal geen informatie opslaat. In plaats daarvan worden wachtwoorden gegenereerd met behulp van een 'pure function'. Dit is een concept in programmeren waarbij een functie of algoritme altijd exact hetzelfde resultaat geeft zonder bijwerkingen, mits je dezelfde invoer geeft. De functie wordt altijd berekend op je eigen systeem, waardoor er nooit iets verstuurd wordt naar een server. Als invoer heb je de naam van een website nodig, de loginnaam en je hoofdwachtwoord. Daarnaast kun je nog extra opties kiezen waar het wachtwoord aan moet voldoen. Dit is eigenlijk hetzelfde als een traditionele wachtwoordmanager, maar het gebruikt de naam van de website, je loginnaam en je hoofdwachtwoord samen om een uniek wachtwoord te genereren.
Het grootste probleem met dit systeem is dat je voor iedere website de specifieke opties moet onthouden, als je niet de standaardopties gebruikt. Dit is juist het probleem dat we proberen op te lossen met een wachtwoordmanager. LessPass lost dit op door ook de optie te bieden om een account aan te maken waar al die opties voor al je accounts worden opgeslagen. Hiervoor kun je de publieke online LessPass server gebruiken, maar je kunt die server ook zelf opzetten, omdat alle code open-source (publiek beschikbaar) is. Doordat deze methode fundamenteel anders is dan de andere wachtwoordmanagers, biedt LessPass ook niet dezelfde extra functies als de andere wachtwoordmanagers.

Conclusie

In dit artikel zijn veel functies belicht die bekende wachtwoordmanagers bieden. Deze functies kunnen het inloggen bij diensten gemakkelijker maken, maar ze kunnen je accounts ook minder veilig maken. Het is belangrijk om zelf deze overwegingen te maken en ik hoop dat je met de kennis uit dit artikel een weloverwogen beslissing kunt nemen. Houd in gedachten dat de kernfunctie van een wachtwoordmanager het veilig opslaan van wachtwoorden is. Uiteindelijk is de beste wachtwoordmanager degene die je gemakkelijk kunt gebruiken en degene die je vertrouwt om jouw accounts veilig te houden.

[1] Noot van de redactie:
In zijn column in deze uitgave van IB Magazine gaat Lex Borger in op het fenomeen passwordmanagers en de hack van LastPass vorig jaar. Dit onder de kop 'Password mismanagement'. Lees zeker deze column op pagina 23 (nog) eens wanneer je op het punt staat een keuze te maken voor een wachtwoordmanager.