Met een wachtwoordbeheerder kun je al je inloggegevens veiligstellen in een digitale kluis. Naast bekende toepassingen als LastPass en 1Password is er de gratis wachtwoordmanager Bitwarden. Dat is een populair en snelgroeiend opensource alternatief dat snel en eenvoudig werkt. Lees hier wat je er zoal mee kunt.

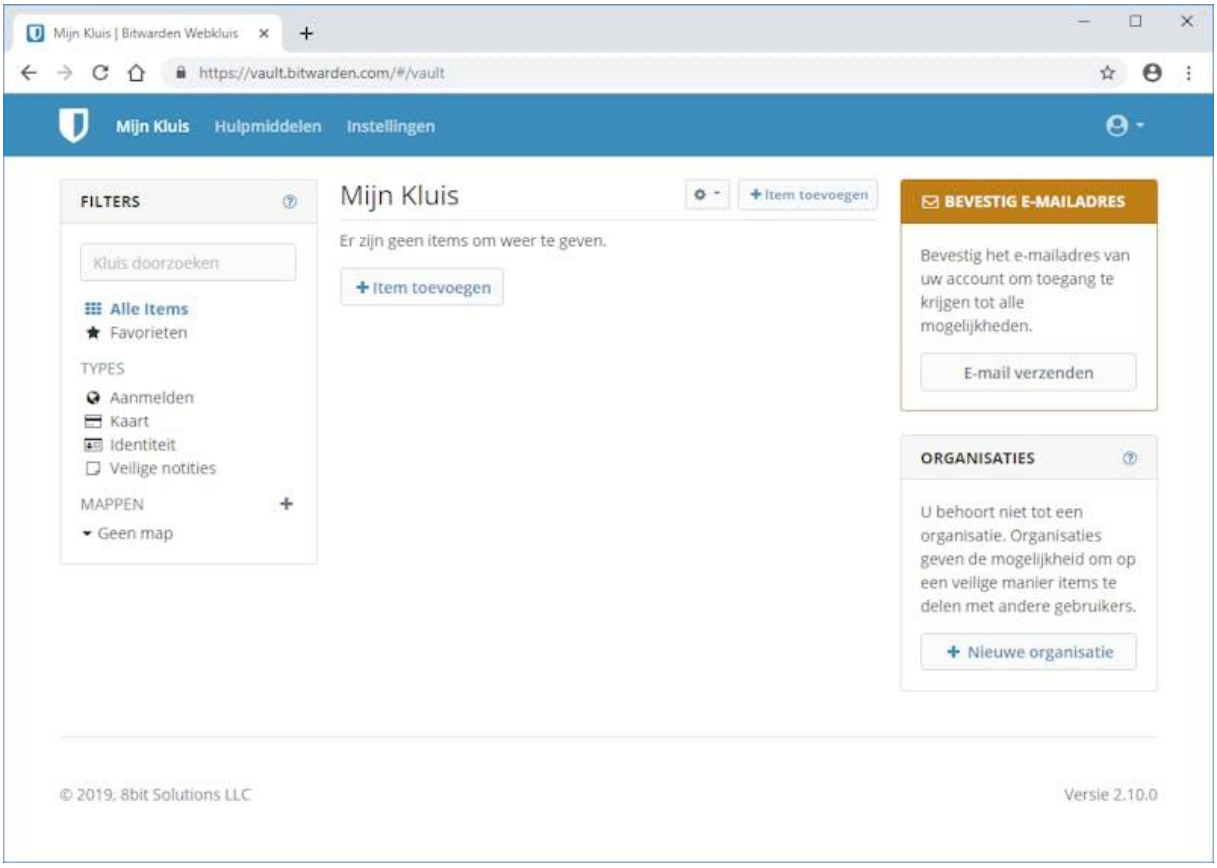
Een wachtwoordbeheerder is een erg praktisch hulpmiddel voor het bewaren van accounts en andere belangrijke gegevens. Je kunt vanaf al je apparaten toegang krijgen tot die gegevens terwijl je slechts één hoofdwachtwoord of pincode hoeft te onthouden. Een extra voordeel is dat je moeiteloos unieke en extra sterke wachtwoorden kunt creëren. Je hoeft ze immers toch niet zelf te onthouden. Naast bekende spelers als LastPass, Dashlane, 1Password en Roboform komt er af en toe een aantrekkelijke nieuwkomer langs. Zoals Bitwarden, dat al veel gebruikers wist weg te lokken bij vooral LastPass. Wellicht omdat LastPass sinds de overname door LogMeIn veel duurder is geworden zonder echt wat toe te voegen.

Een meerwaarde van Bitwarden is dat het opensource is en dus niets kan verbergen, behalve natuurlijk je zorgvuldig versleutelde wachtwoorden. Ook blijkt de wachtwoordbeheerder erg gebruiksvriendelijk. Laten we aan de slag gaan!

Hoofdwachtwoord instellen en kluis verkennen.

We maken om te beginnen een persoonlijk gebruikersaccount. Ga naar de site van Bitwarden en klik op **Create Account**. Voer je e-mailadres, naam en een (sterk) hoofdwachtwoord in. Dat is het wachtwoord waarmee je toegang krijgt tot de beveiligde kluis. Op basis van dit wachtwoord worden al je inloggegevens versleuteld met een krachtig algoritme. Op de servers van het bedrijf worden je gegevens óók in versleutelde vorm bewaard, zodat ze (bijvoorbeeld bij een data-lek) feitelijk onbruikbaar zijn zonder dat hoofdwachtwoord.

Log na het maken van het account in om in de zogenaamde Web Vault te komen, je (nu nog lege) digitale kluis. Kies rechtsboven, onder **Bevestig e-mailadres**, de optie om een verificatielink naar je e-mailadres te sturen. Via die link kun je het e-mailadres bevestigen en – na opnieuw inloggen – alle mogelijkheden van Bitwarden benutten.



In de Web Vault kun je, op het tabblad **Mijn Kluis**, de items in de digitale kluis beheren, zoals je inloggegevens (**Aanmelden**), creditcardgegevens (**Kaart**), persoonlijke gegevens (**Identiteit**) en notities (**Veilige notities**). Je kunt onbeperkt gegevens toevoegen en zelfs onbeperkt synchroniseren met andere apparaten zoals smartphones, tablets en pc's. Het bijwerken gebeurt voor het grootste deel ongemerkt op de achtergrond zodra je iets wijzigt.

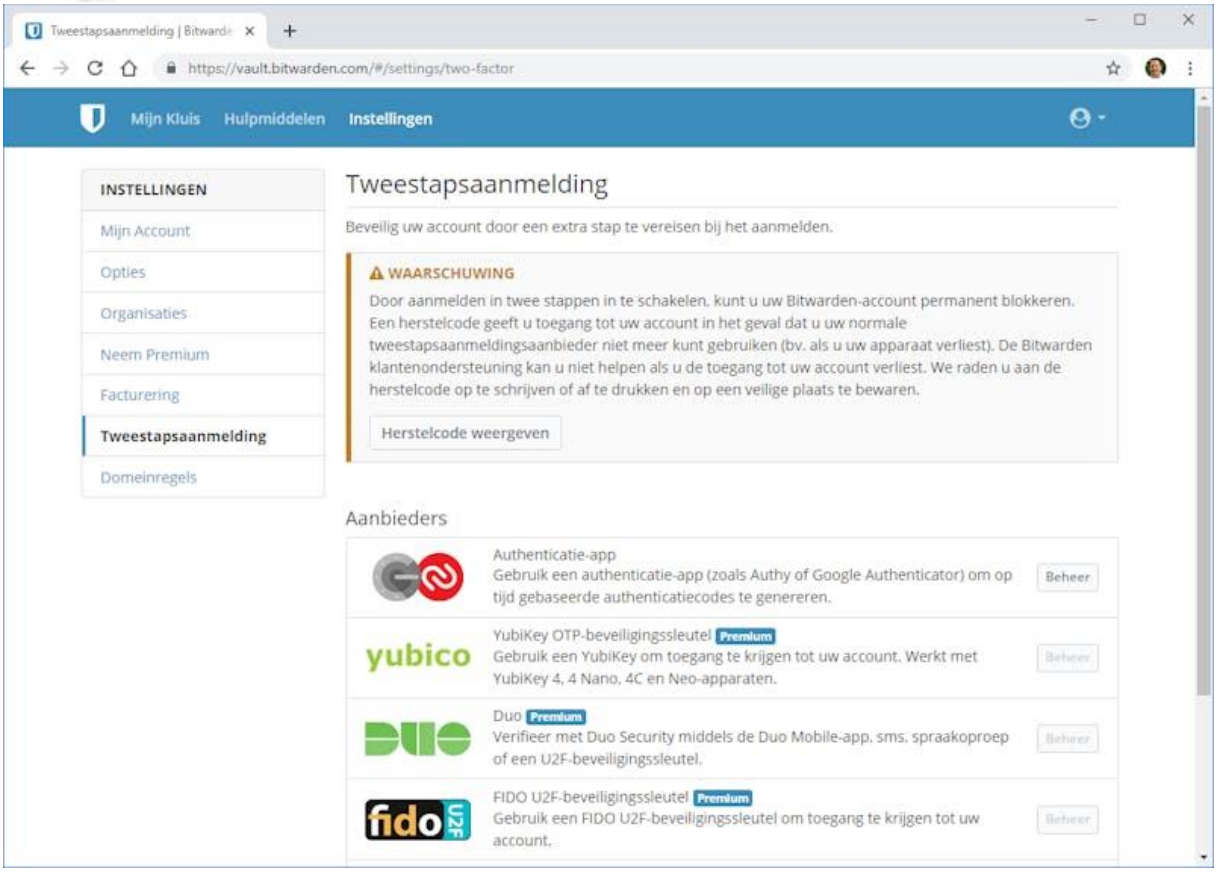
Gebruik je reeds een andere wachtwoordbeheerder, zoals LastPass of Roboform? Dan kun je op het tabblad **Hulpmiddelen** de gegevens van talloze wachtwoordbeheerders importeren, nadat je ze eerst vanuit de bestaande wachtwoordbeheerder hebt geëxporteerd. Wat natuurlijk ook kan, is dat je ze een tijdje naast elkaar gebruikt en wachtwoorden op het moment dat je ze nodig hebt overneemt. Dat schoont ook de vaak lange lijst met deels overbodig geworden inloggegevens weer een beetje op.

Verder kun je op dit tabblad de gegevens van Bitwarden zelf exporteren. Pas wel op, want zo'n exportbestand bevat je leesbare wachtwoorden. De rapportages die je hier kunt inzien zijn overigens alleen beschikbaar met een Premium-account (waarover straks meer).

Je kunt behalve via de Web Vault uiteraard ook met andere toepassingen toegang krijgen tot de digitale kluis. Zo zijn er desktoptoepassingen voor Windows, macOS of Linux die vooral handig zijn voor het beheren van de opgeslagen gegevens. Ook zijn er extensies voor alle bekende browsers, waaronder Chrome en Firefox. Daarmee kun je onder andere tijdens het browsen automatisch inloggen in je accounts, maar ook gemakkelijk nieuwe inloggegevens in de kluis opslaan. Verder zijn er zowel voor Android als iOS (iPhone en iPad) apps beschikbaar die helpen bij het invullen van wachtwoorden op deze apparaten.

Tweestapsverificatie instellen.

Hierna is het slim om de toegang af te schermen met tweestapsverificatie. Hiervoor ga je naar het tabblad **Instellingen** en dan **Tweestapsaanmelding**. Klik dan achter **Authenticatie-app** op **Beheer**. Vul nu je hoofdwachtwoord in. Hierna zie je een qr-code. Open een app als Google Authenticator of Authy, kies daarin de optie om een account toe te voegen en scan de qr-code. De app zal dan een eerste toegangscode genereren die je overneemt in de Web Vault om tweestapsverificatie definitief aan te zetten.



In het vervolg zul je op elk nieuw apparaat waarop je de Web Vault - of een van de andere toepassingen van Bitwarden - gaat gebruiken, een toegangscode moeten invullen. Daarvoor moet je dus even de smartphone met de app erbij pakken.

Tip: bewaar de herstelcode die je via **Instellingen, Tweestapsaanmelding** kunt weergeven, om te voorkomen dat je wordt buitengesloten als je bijvoorbeeld je smartphone verliest!

Bitwarden Premium-voordelen.

We hebben nu in een notendop de belangrijkste features van het gratis account van Bitwarden behandeld. Voor de meesten zijn dit meer dan genoeg functies, maar wie dat wil kan een upgrade naar Premium overwegen. Een upgrade naar Premium ($ 10/jaar) kan in sommige situaties aantrekkelijk zijn. Zo kun je daarmee dankzij 1 GB versleutelde bestandsopslag bijlagen toevoegen aan items in de kluis, bijvoorbeeld een foto van je creditcard.

Ook biedt Premium extra mogelijkheden om in te loggen met tweestapsverificatie voor je kluis zelf. Daarnaast geeft Premium de mogelijkheid verificatiecodes te genereren voor accounts die met tweestapsverificatie zijn afgeschermd, zoals Dropbox en GitHub, waarbij feitelijk de rol van Google

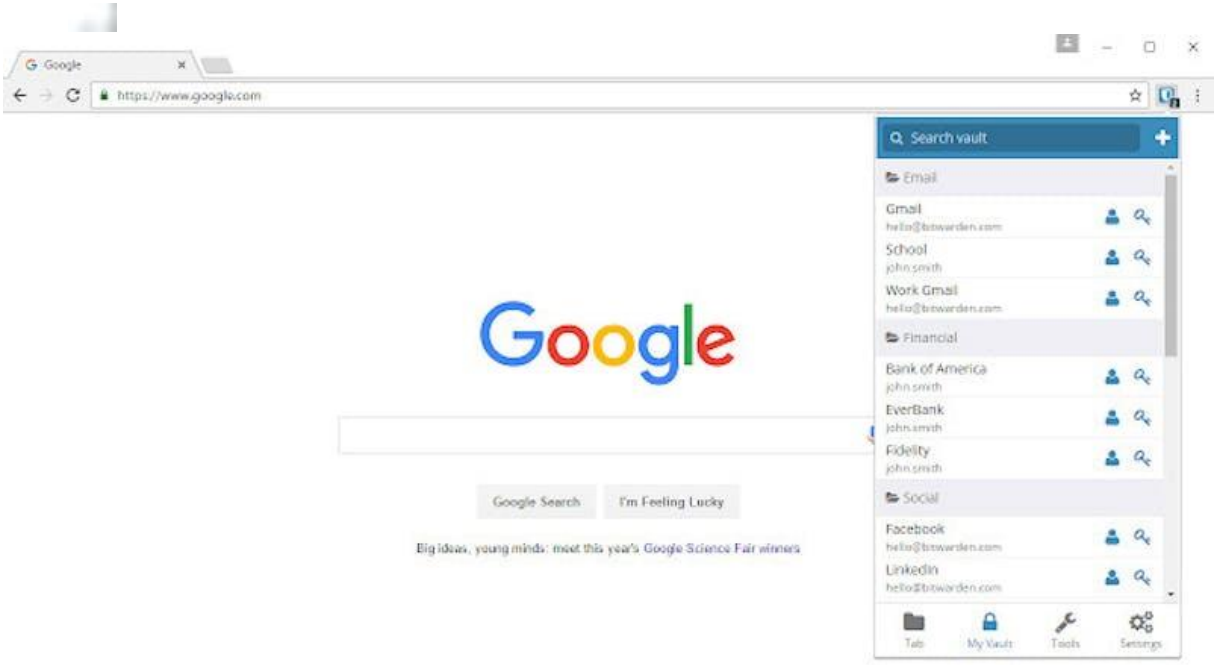
Authenticator wordt overgenomen. Verder krijg je via rapporten advies over je wachtwoordgebruik, ter voorkoming van blootgestelde, dubbele of zwakke wachtwoorden.

Regelmatig back-ups maken van je belangrijke bestanden, raden we iedereen aan. Toch schiet het er geregeld bij in. Neem een kijkje bij onze Cursus Back-up en herstel, vol tips voor Windows, macOS, Android en iOS. Eventueel met 180 pagina's tellend praktijkboek!

Bitwarden-extensies.

Bij een wachtwoordbeheerder hoort natuurlijk een goede browserextensie. Bitwarden heeft dat goed voor elkaar. Behalve voor Chrome en Firefox biedt het ook extensies voor Safari, Opera, Microsoft Edge, Vivaldi en Brave. We nemen Bitwarden voor Chrome als voorbeeld. Klik op de button **Toevoegen aan Chrome**. Hiermee wordt het icoontje van Bitwarden aan je browser toegevoegd. Klik op het icoontje, kies **Inloggen** en vul je inloggegevens in. Als je tweestapsverificatie hebt aangezet is ook een toegangscode nodig.

Het is handig de optie **Mijn gegevens onthouden** aan te zetten. Ga na het inloggen naar het tabblad **Instellingen** en kies onder **Beveiliging** wanneer het account moet worden vergrendeld. Bijvoorbeeld na een bepaalde tijd, na het herstarten van de browser of nooit. Die laatste optie gebruik je alleen op een apparaat waar anderen geen toegang toe hebben. Verder kun je ervoor kiezen om te ontgrendelen met pincode in plaats van het hoofdwachtwoord, wat in de praktijk vaak makkelijker en sneller werkt.



Als je inlogt bij een bepaalde website waarvoor nog geen account in Bitwarden bestaat, zal het programma via een balk aan de bovenzijde van de browser vragen of het de inloggegevens moet bewaren in de kluis. Werkt die herkenning een keer niet, dan blijft de vraag achterwege, maar kun je (via de optie **Login toevoegen**) de inloggegevens wel handmatig toevoegen. Herkenning voor een website kun je eventueel wat fijner afstellen, zoals het gedeelte van de link waar het naar moet kijken. Waar dat nodig is, kun je inloggegevens met een extra veld uitbreiden (bijvoorbeeld een lidmaatschapsnummer).

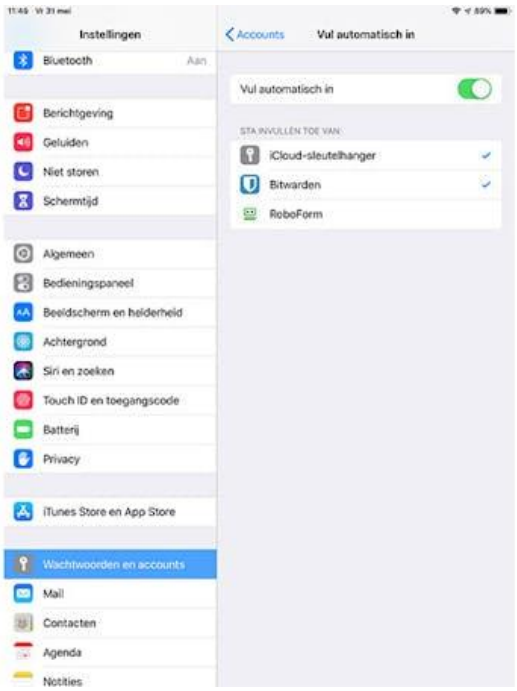
Als Bitwarden bij het inloggen een account vindt in de kluis, zie je dat aan het icoontje, dat met een cijfer het aantal overeenkomende accounts aangeeft. Ook handig om te weten is dat de browserextensie een wachtwoord voor je kan generen voor een account. En mocht je het wachtwoord van een account wijzigen, dan vraagt Bitwarden of het de gegevens in de digitale kluis moet bijwerken.

Wat ten slotte ook heel praktisch is zijn de aan te maken identiteiten, zodat je bijvoorbeeld automatisch formulieren kunt invullen met je adresgegevens en telefoonnummer.

Bitwarden op smartphones (Android, iOS).

Voor zowel Android als iOS (iPhone en iPad) heeft Bitwarden een goedwerkende app beschikbaar. We nemen de iPad als voorbeeld. Na het inloggen met je account en eenmalig – als je tweestapsverificatie hebt aangezet – de toegangscode, krijg je toegang tot alle items in de digitale kluis. In het vervolg kun je toegang eventueel met een pincode afschermen.

De kluis wordt automatisch up-to-date gehouden met de hulp van pushnotificaties. Zodra je op een ander apparaat een wachtwoord toevoegt of wijzigt, staat het dus ook op je iPad.



Bij het inloggen in accounts via de browser helpt Bitwarden natuurlijk ook. Dit is onlangs verbeterd dankzij een nieuwe voorziening in iOS 12. Wachtwoorden kunnen nu direct vanaf het toetsenbord worden ingevuld. Om het te activeren open je **Instellingen**, tik op **Wachtwoorden & Accounts** en dan **Vul automatisch in**. Zet de optie aan en kies in het lijstje voor Bitwarden. Bevestig met je hoofdwachtwoord. Hierna kun je tijdens het browsen snel en eenvoudig inloggen.

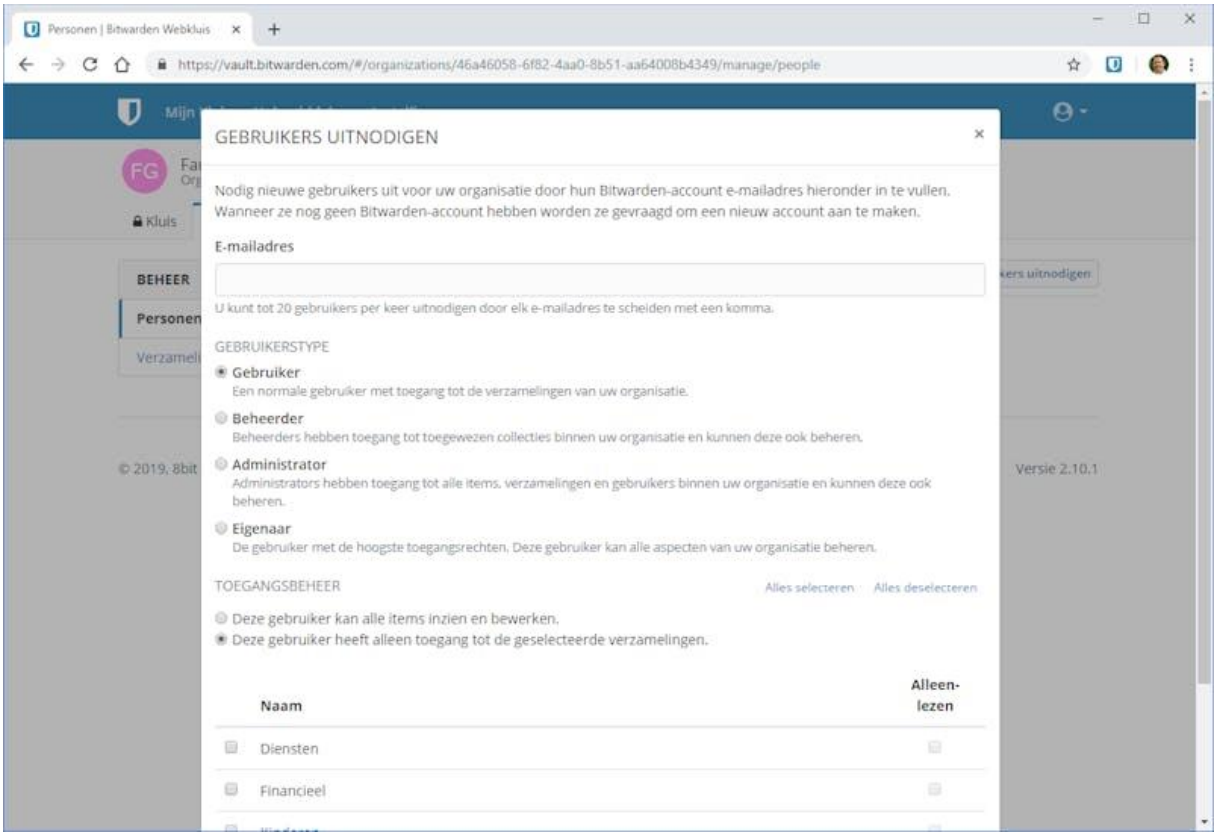
Bij Android 8 in enkele browsers, en sinds Android 9 in nog veel meer browsers, gaat dat ongeveer hetzelfde. De toegankelijkheidsvoorzieningen die hiervoor werden gebruikt (of eigenlijk misbruikt) zijn daardoor niet meer nodig.

Wachtwoorden delen.

In bedrijven maar ook in een gezinssituatie zal het vaak voorkomen dat je bepaalde gegevens onderling wilt delen, bijvoorbeeld inloggegevens voor de internetprovider of een veilige notitie met spaartegoeden of softwarelicenties. Dit kan met Bitwarden heel eenvoudig. Om het in te stellen ga je naar de Web Vault en dan naar **Instellingen**. Kies **Organisaties**.

Bij het gratis pakket kun je gegevens met twee gebruikers delen en twee verzamelingen aanmaken, om gegevens logischer in te kunnen delen. Het pakket voor families kost een dollar per maand en staat het delen met maximaal vijf gebruikers toe en onbeperkte verzamelingen. Daarmee kun je tevens tot 1 GB aan bijlagen toevoegen aan items die in de organisatie worden gedeeld.

Verder zijn er nog enkele zakelijke pakketten. Zo'n organisatie staat overigens helemaal los van de Premium-accounts. Elke individuele gebruiker van de organisatie kan zelf kiezen voor de extra's van Premium, maar dat is geen verplichting.



Heb je een organisatie gemaakt en wil je die beheren, ga dan weer naar **Instellingen, Organisaties** en klik op de naam van de organisatie. Hierna kom je in het beheergedeelte voor de organisatie. Via tabjes kun je naar **Kluis** met alle gedeelde items en **Beheer** waar je gebruikers kunt uitnodigingen voor de organisatie. Hierbij kun je kiezen welke rechten en beperkingen er zijn voor die gebruiker, zoals de verzamelingen waar ze toegang toe hebben.

De verzamelingen kun je in dit onderdeel ook bewerken. Het delen van items met de organisatie gaat hierna eigenlijk eenvoudig. In je eigen kluis zie je bij elk item een optie om die te delen met de organisatie, waarna die organisatie in feite eigenaar van het item wordt. Elke wijziging wordt bij de leden van de organisatie doorgevoerd.

Zelf hosten.

Tot slot. Er is weinig op tegen om Bitwarden te gebruiken via de standaard servers van het bedrijf. Weliswaar worden je wachtwoorden daar opgeslagen, maar alleen in versleutelde vorm, wat ze waardeloos maakt zonder je hoofdwachtwoord. Als je dat toch niet helemaal vertrouwt en ervaring hebt met het zelf hosten van toepassingen, kun je Bitwarden ook op een eigen server hosten. Die server moet wel over relatief veel geheugen beschikken (minimaal 2 GB).

Er is met Bitwarden-rs (afgeslankte versie van officiële server) overigens ook een lichtgewicht (en eveneens opensource) alternatief dat door derden is ontwikkeld. Die biedt vrijwel alle functies en ondersteunt gewoon de standaard toepassingen van Bitwarden, zoals de browserextensies. Het maken van een organisatie kan zelfs zonder meerprijs en verdere beperkingen.