**Stap 1: Gratis Back-up Plugin Installeren en Configureren**

**Plugin Suggestie: BackWPup**

BackWPup is een gratis en krachtige plugin waarmee je eenvoudig automatische back-ups kunt instellen. Het ondersteunt opslag op verschillende locaties, zoals Dropbox of een lokale server.

**Installatie**

1. Log in op je WordPress-dashboard.
2. Ga naar **Plugins** > **Nieuwe plugin**.
3. Zoek naar **BackWPup**.
4. Klik op **Nu installeren** en vervolgens op **Activeren**.

**Configuratie**

1. Ga naar **BackWPup** > **Nieuwe taak toevoegen**.
2. Stel de volgende opties in:
   * **Naam van de taak**: Wekelijkse back-up.
   * **Taken**: Vink aan **Database back-up** en **Bestanden back-up**.
   * **Opslaglocatie**: Kies een gratis optie, zoals **DropBox** of **Opslag op server**.
3. Klik op **Opslaan**.
4. Ga naar het tabblad **Planning**:
   * Kies **WordPress Cron**.
   * Stel in op **Wekelijks**.
   * Selecteer een dag en tijdstip (bijvoorbeeld zondag om 03:00 uur).
5. Ga naar het tabblad **Bestemming**:
   * Configureer je opslaglocatie (bijvoorbeeld een lokale server of Dropbox).
   * Volg de instructies voor de verbinding met een externe opslag (zoals een API-sleutel voor Dropbox).
6. Ga naar het tabblad **Bestandsbehoud**:
   * Stel het aantal back-ups in op maximaal **4**.
7. Klik op **Opslaan**.

**Stap 2: Gratis Beveiligingsplugin Installeren en Configureren**

**Plugin Suggestie: All In One WP Security & Firewall**

Deze gratis plugin biedt een uitgebreide beveiliging met brute force-bescherming, firewall-opties en malware-detectie.

**Installatie**

1. Ga naar **Plugins** > **Nieuwe plugin**.
2. Zoek naar **All In One WP Security & Firewall**.
3. Klik op **Nu installeren** en vervolgens op **Activeren**.

**Configuratie**

1. Ga naar **WP Security** > **Dashboard**:
   * Controleer de "Security Strength Meter" om te zien hoeveel beveiliging er is geactiveerd.
2. **Brute Force-bescherming**:
   * Ga naar **Brute Force** > **Login Lockdown**.
   * Schakel de optie in en stel in:
     + Maximaal aantal inlogpogingen: 3.
     + Lockout tijd: 30 minuten.
3. **Firewall**:
   * Ga naar **Firewall** > **Basis firewallregels**.
   * Schakel de basisregels in (zoals "Blokkeer toegang tot onnodige bestanden").
4. **Blokkeer verdachte IP's**:
   * Ga naar **Blacklist Manager**.
   * Voeg handmatig verdachte IP-adressen toe of gebruik automatische regels.
5. **Scans**:
   * Ga naar **File Change Detection**.
   * Schakel meldingen in als bestanden onverwacht worden gewijzigd.

**Stap 3: Testen**

**Back-up testen**

1. Ga naar **BackWPup** > **Takenlijst**.
2. Klik op **Uitvoeren** bij de gemaakte taak.
3. Controleer of de back-up is opgeslagen op de juiste locatie.

**Beveiliging testen**

1. Controleer of de firewall werkt door naar de instellingen te gaan in **WP Security**.
2. Simuleer meerdere foutieve aanmeldpogingen om te zien of brute force-bescherming werkt.

Met **BackWPup** en **All In One WP Security & Firewall** heb je een volledig gratis oplossing die wekelijkse back-ups maakt (tot vier versies bewaart) en je website beschermt tegen hackpogingen.