iThemes Security

Wordpress-Plugin - Datensicherheit

Dieses Sicherheits-Plugin soll Ihre Website noch sicherer machen. Wenn Sie meiner Empfehlung gefolgt sind und WPS Hide Login installiert haben, sind Sie einen sehr großen Teil Ihrer Angreifer los, da diese gar nicht den Eingang zu Ihrem Administrationsbereich finden. Um aber den ganz hartnäckigen Hackern das Leben noch schwerer zu machen, sollten Sie iThemes Security zusätzlich installieren.

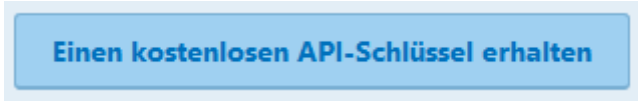
Weitere Informationen:
https://de.wordpress.org/plugins/better-wp-security/

---

iThemes Security – Downloaden und Installieren

1. Rufen Sie den Administrationsbereich (Dashboard) Ihrer Wordpress-Installation auf.
2. Klicken Sie in der linken Navigationsleiste auf *Plugins* – es werden Ihre installierten Plugins angezeigt.
3. Klicken Sie auf den Button (oben neben Plugins) *Installieren.*
4. Es wird Ihnen eine Übersicht der Plugins angezeigt, die Wordpress zur Verfügung stellt.
5. Geben Sie rechts oben als Stichwort in das Suchfeld *iThemes* ein.
6. Danach zeigt Wordpress Ihnen das Plugin an erster Stelle der Übersicht.

7. Klicken Sie auf *Jetzt installieren* – nach der Installation auf *Aktivieren.*



Klicken Sie auf diesen Button. Bei einer Neu-Installation wird Ihre E-Mail-Adresse gespeichert. Den API-Schlüssel erhalten Sie per E-Mail zugesandt. Diesen müssen Sie in das entsprechende Eingabefeld einfügen.

iThemes Security - Login und Einrichten

1. iThemes Security wird in Ihrer Plugin-Übersicht angezeigt. Außerdem finden Sie einen neuen Button *Sicherheit* in der linken Navigationsleiste.

2. Klicken Sie auf *Sicherheit* > *Einstellungen.*

3. Es öffnet sich als erstes die *Sicherheitsüberprüfung.*
   Das Plugin schlägt jetzt schon ein paar Einstellungen vor. Nehmen Sie den Vorschlag an und klicken auf *Secure Site.* Das sind alles passende Einstellungen. Wir werden noch einige anpassen, aber dazu später.

4. Danach erscheint eine Bestätigungsübersicht aller vorbereiteten Einstellungen.
   Wenn Sie möchten, können Sie regelmäßig über Neuerungen zum Plugin informiert werden.

   Geben Sie dazu Ihre E-Mail-Adresse ein und bestätigen Sie den Netzwerk-Brut-Force-Schutz. Anschließend erhalten Sie eine Bestätigung per E-Mail.
   Klicken Sie danach auf *Schließen.*

5. Die Übersichtsseite wird angezeigt. Damit alles übersichtlicher wird, klicken Sie oben neben Module auf den *Listen-Button*. Jetzt werden die einzelnen Bereiche aufgelistet und lassen sich so leichter bearbeiten.

   Die Entwickler von iThemes Security schlagen auch vor die Pro-Version zu kaufen, aber das ist nicht notwendig. Die wichtigsten Funktionen bietet auch die kostenlose Version.

6. **Globale Einstellungen**
   Hier werden Ihnen einen ganze Liste von Einstellmöglichkeiten angezeigt. Vieles ist selbsterklärend – bitte durchlesen. Ich empfehle, alle Grundeinstellungen unverändert zu lassen, mit Ausnahme:
   Weiße Liste – Entriegelung:
   Klicken Sie auf *Meine derzeitig IP der weißen Liste hinzufügen.*
   Dadurch wird Ihre eigene Website nicht ausgesperrt.
   Einstellungen speichern.

7. **Benachrichtigungszentrale**
   Hier werden die E-Mail-Benachrichtigungen eingestellt. Viele Einträge können gelöscht werden, da sonst sehr viele – zum Teil unnötige - E-Mails an Sie gesendet werden.
   Default Recipients > Haken kann entfernt werden
   Dateiänderung > Haken kann entfernt werden
   Sicherheitsbericht > Haken kann entfernt werden
   Website-Aussperrungen >Haken kann entfernt werden
   Falls Sie aber diese Informationen wünschen können, Sie auch die Haken stehen lassen.
   Einstellungen speichern.

8. **404-Erkennung**
   Diese Einstellung sollte aktiviert werden. Die Grundeinstellung kann unverändert bleiben.
   Einstellungen speichern.

9. **Abwesenheitsmodus**
   Die Aktivierung ist nicht nötig. Weitere Informationen können Sie dort lesen.

10. **Benutzersperrung**
    Vorgegebene Schwarze Liste > Haken setzen
    So werden schon im Vorfeld bekannte Hacker gesperrt.
    Sperrlisten aktivieren – hier könnten IP-Adressen von „bösen Buben“ eingefügt werden.
    Einstellungen speichern.

11. **Datenbank-Backup**
    Deaktivieren, wenn Sie bereits UpdraftPlus installiert haben oder dieses beabsichtigen.

12. **Dateiänderungserkennung**
    Aktivieren. Falls eine Ihrer Dateien geändert wurde, wird dies im Sicherheitsbericht protokolliert.

13. **Dateiberechtigungen**
    Nichts verändern.

14. **Lokaler Brute-Force-Schutz**
    Gut eingestellt – nichts ändern – aber durchlesen und überprüfen.
    Ausnahme: Bei „Admin-Benutzer automatisch sperren“ - Haken setzen.
    So kann sich niemand mehr mit dem Benutzer-Namen „Admin“ anmelden -
    denn das ist oft das erste, was Hacker versuchen.

15. **Netzwerk Brute-Force-Schutz**
    Nichts ändern, der API-Schlüssel wurde bei der Installation automatisch eingetragen.

16. **SSL**
    Aktivieren - falls SSL eingesetzt wird.

17. **Sichere Passwörter erzwingen**
    Sichere Passwörter sind gut, aber auch lästig. Ich empfehle, keinen Haken zu setzten.
    Wenn Sie es trotzdem wünschen … Haken setzen – *Minimun Role > Administrator.*
    Beachten Sie dabei, wenn der Haken gesetzt ist, fordert das Plugin in Abständen neue Passwörter an, die dann immer notiert und bei Bedarf an mich (Webmaster) gesendet werden müssen. Sonst habe ich keinen Support-Zugriff mehr.

18. **System-Optimierungen**
    Durchlesen und bei Bedarf aktivieren.

19. **WordPress-Salt-Werte (Sicherheitsschlüssel)**
    Durchlesen – nur bei Bedarf Haken setzen.

20. **WordPress-Optimierungen**
    Durchlesen - nur bei Bedarf Haken setzen.

Die weiteren Einträge (PRO) werden nur nach dem Erwerb der PRO-Version freigeschaltet.
Den 100%igen Schutz gibt es für keine Webseite.
Auch wenn Sie den Inhalt Ihres Internetauftritts ändern, sollten Sie regelmäßig den Admistrationsbereich aufrufen, auf Änderungen hin überprüfen und Aktualisierungen durchführen.