04.D2

CHECKLISTE

WORDPRESS ABSICHERN: DIE WICHTIGSTEN SCHRITTE

Lesezeit:	4 Minuten
Niveau:	Fachwissen
Ziel:	Die WordPress-Website mit zehn einfachen Schritten gegen die häufigsten Angriffe absichern.
Veröffentlicht:	05/2026
Aktualisiert:	-

WORDPRESS IST BELIEBT – AUCH BEI HACKERN.

30 Prozent aller Websites laufen auf WordPress, das macht das Content-Management-System zu einem attraktiven Ziel für Angriffe. Diese Checkliste zeigt Ihnen zehn einfache Schritte, mit denen Sie 90 Prozent der Angriffe abwehren.

⚠️ **Wichtig**: Ohne technische Vorkenntnisse sollten Sie die Absicherung nicht selbst durchführen. Der Prozess setzt Folgendes voraus:

- Sie sind mit den Grundlagen der WordPress-Verwaltung vertraut
- Sie haben Zugriff auf das Backend und auf den Server, etwa per FTP
- Sie können Plugins installieren, konfigurieren und Einstellungen anpassen
- Sie kennen sich mit Dateiberechtigungen und der *.htaccess*-Datei aus
- Sie können ein Backup erstellen und im Ernstfall wiederherstellen

Sind Sie sich bei einem dieser Punkte unsicher, holen Sie sich Unterstützung.

Inhalt

SCHRITT 1: ADMIN-BENUTZERNAMEN ÄNDERN

☐ **Ändern Sie den Standard-Benutzernamen:**

- Keinen Benutzernamen "admin" verwenden
- Keinen offensichtlichen Benutzernamen verwenden, etwa den Firmennamen
- Eine Kombination aus Buchstaben und Zahlen einsetzen

SCHRITT 2: STARKE PASSWÖRTER VERWENDEN

☐ **Verwenden Sie durchgehend starke Passwörter:**

- Mindestens 16 Zeichen
- Groß- und Kleinbuchstaben
- Zahlen und Sonderzeichen
- Keine Wörter aus dem Wörterbuch
- Passwort-Manager nutzen, etwa 1Password oder ProtonPass

🧩 **Praxisbeispiel**: Ein schlechtes Passwort ist *Schmidt123!*, ein gutes Passwort ist *K9mP2$vL8@nQ4xZ*.

⚠️ **Wichtig:** Wer dasselbe Passwort mehrfach verwendet, riskiert bei einem einzigen kompromittierten Konto den Zugang zu allen anderen.

SCHRITT 3: 2FA NUTZEN

☐ **Richten Sie die Zwei-Faktor-Authentifizierung (2FA) ein:**

- 2FA-Plugin installieren
- 2FA für Admin-Konto aktivieren
- Backup-Codes für die 2FA sicher aufbewahren

SCHRITT 4: LOGIN-VERSUCHE BEGRENZEN

☐ **Begrenzen Sie die Anzahl der Login-Versuche:**

- Plugin installieren, etwa Limit Login Attempts Reloaded
- Maximal drei Login-Versuche erlauben
- Sperre nach Fehlversuchen einstellen: 60 Minuten
- E-Mail-Benachrichtigung bei Sperren aktivieren

⚠️ **Wichtig:** Angreifer testen automatisiert tausende Passwörter durch – sogenannte Brute-Force-Attacken. Begrenzte Login-Versuche erschweren das, ersetzen aber keine weiteren Schutzmaßnahmen.

SCHRITT 5: WORDPRESS UND PLUGINS AKTUELL HALTEN

☐ **Halten Sie WordPress und alle Erweiterungen aktuell:**

- Automatische Updates für WordPress-Kern aktivieren
- Erweiterungen manuell oder automatisch aktualisieren
- Layout-Vorlage (Theme) aktuell halten
- E-Mail-Benachrichtigung für verfügbare Updates aktivieren

💡 **Tipp:** 60 Prozent der gehackten WordPress-Websites hatten veraltete Erweiterungen. Updates sind keine optionale Maßnahme.

SCHRITT 6: UNGENUTZTE PLUGINS LÖSCHEN

☐ **Räumen Sie nicht genutzte Erweiterungen konsequent auf:**

- Liste aller installierten Plugins durchgehen
- Ungenutzte Plugins deaktivieren
- Deaktivierte Plugins löschen, nicht nur deaktivieren

⚠️ **Wichtig:** Jedes Plugin ist eine potenzielle Sicherheitslücke – auch wenn es deaktiviert ist.

🧩 **Praxisbeispiel:** Ein Kunde hatte 47 Erweiterungen installiert, zwölf davon aktiv ge-

nutzt. Die anderen 35 waren ungenutztes Angriffspotenzial.

SCHRITT 7: SSL-VERSCHLÜSSELUNG AKTIVIEREN

☐ **Aktivieren Sie die SSL-Verschlüsselung:**

- SSL-Zertifikat beim Hoster bestellen
- WordPress auf *https://* umstellen
- Weiterleitungen von *http://* auf *https://* einrichten

📌 **Merke:** Ohne *https://* werden Passwörter und Formulardaten unverschlüsselt übertragen. Google bewertet Websites ohne *https://* schlechter.

SCHRITT 8: DATENBANKPRÄFIX ÄNDERN

☐ **Ändern Sie das Datenbankpräfix:**

- Nicht das Standardpräfix *wp_* verwenden
- Ein eigenes Präfix setzen, etwa *mf7_* oder *ac_*

⚠️ **Wichtig:** Angriffsskripte zielen standardmäßig auf Tabellennamen wie *wp_users*. Ein geändertes Präfix macht diese Angriffe wirkungslos. Das Präfix lässt sich nur bei der Installation setzen – eine nachträgliche Änderung ist technisch aufwendig und sollte einem Experten überlassen werden.

SCHRITT 9: FIREWALL INSTALLIEREN

☐ **Richten Sie eine Firewall ein:**

- Sicherheitssoftware installieren, etwa Wordfence, Sucuri oder iThemes Security
- Firewall aktivieren
- Malware-Scan einrichten
- E-Mail-Benachrichtigung bei verdächtigen Aktivitäten aktivieren

SCHRITT 10: REGELMÄSSIGE BACKUPS

☐ **Richten Sie regelmäßige Backups ein:**

- Erweiterung für Sicherheitskopien installieren, etwa UpdraftPlus oder BackWPup
- Automatische Backups einrichten
- Externen Backup-Speicherort nutzen
- Backup-Wiederherstellung testen

ZUSÄTZLICHE SICHERHEITSTIPPS

☐ **Folgende Maßnahmen bieten zusätzlichen Schutz:**

- Login-URL ändern – der Standardpfad */wp-admin* ist jedem Angreifer bekannt
- Datei-Berechtigungen prüfen – *wp-config.php* sollte 440 oder 400 haben, nicht 777
- *xml-rpc.php* über *.htaccess*-Datei deaktivieren – wird regelmäßig für Angriffe missbraucht
- Admin-Bereich per IP beschränken, sodass nur freigegebene Adressen Zugang zum Login erhalten

DIE DREI HÄUFIGSTEN FEHLER

- **„Mir passiert das nicht“** – Angriffe sind automatisiert. Jede Website ist ein potenzielles Ziel, unabhängig von Größe oder Bekanntheit.
- **Sicherheit einmalig einrichten, dann vergessen** – Sicherheit ist kein Zustand, sondern ein laufender Prozess. Regelmäßige Prüfung ist Pflicht.
- **Zu viele Sicherheitserweiterungen** – ein bis zwei durchdachte Lösungen reichen aus. Mehr bremsen die Website, ohne zusätzlichen Schutz zu bieten.

WORAN SIE MERKEN, DASS SIE ANGEGRIFFEN WURDEN

Folgende Warnsignale deuten auf einen erfolgreichen Angriff hin:

- Website lädt plötzlich langsam

- Es erscheinen unbekannte Admin-Konten
- Spam-Mails werden von Ihrer Domain verschickt
- Google warnt vor Ihrer Website ("Diese Seite könnte gehackt worden sein")
- Im FTP finden sich Dateien mit seltsamer Benennung, etwa *x.php*

Wenn Sie gehackt wurden:

1. Website sofort offline nehmen
2. Alle Passwörter ändern
3. Backup von vor dem Angriff einspielen
4. Professionelle Bereinigung beauftragen

Eine abgesicherte Website ist keine Garantie – aber sie ist kein leichtes Ziel mehr. **Sie möchten die Sicherheit Ihrer Website nicht selbst einrichten? Ich übernehme die Absicherung für Sie.**

→ Projektanfrage stellen
→ Fragen stellen