02.D2

CHECKLISTE

WORDPRESS ABSICHERN: DIE WICHTIGSTEN SCHRITTE

⏱️ **Lesedauer**: 3-4 Minuten
📊 **Schwierigkeit**: Basiswissen
🎯 **Ziel**: Ihre WordPress-Website gegen die häufigsten Angriffe absichern

📅 **Veröffentlicht:** 05/2026

WORDPRESS IST BELIEBT. AUCH BEI HACKERN.

30% aller Websites laufen auf WordPress – das macht es zum attraktiven Ziel für Angriffe. Diese Checkliste zeigt Ihnen zehn einfache Schritte, mit denen Sie 90% der Angriffe abwehren.

Punkt für Punkt umsetzen. Ruhiger schlafen.

Inhalt

SCHRITT 1: ADMIN-BENUTZERNAMEN ÄNDERN

- ☐ Keinen Benutzernamen "admin" verwenden: wird von Hackern zuerst getestet
- ☐ Keinen offensichtlichen Benutzernamen (z. B. Firmennamen)
- ☐ Kombination aus Buchstaben und Zahlen einsetzen

💡 **Tipp:** Ändern geht über Benutzer > Profil > Benutzername. Oder neuen Admin anlegen, alten löschen.

SCHRITT 2: STARKE PASSWÖRTER VERWENDEN

- ☐ Mindestens 16 Zeichen
- ☐ Groß- und Kleinbuchstaben
- ☐ Zahlen und Sonderzeichen
- ☐ Keine Wörter aus dem Wörterbuch
- ☐ Passwort-Manager nutzen (z. B. 1Password, Bitwarden)

🧩 **Beispiel**: Schlechtes Passwort: Schmidt123! Gutes Passwort: K9mP2$vL8@nQ4xZ.

⚠️ **Wichtig:** Gleiches Passwort für mehrere Seiten = alle Seiten gefährdet, wenn eine gehackt wird.

SCHRITT 3: ZWEI-FAKTOR-AUTHENTIFIZIERUNG (2FA) NUTZEN

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

📝 **Definition:** 2FA = Passwort + Code vom Handy. Selbst wenn jemand Ihr Passwort

kennt, kommt er nicht rein.

SCHRITT 4: LOGIN-VERSUCHE BEGRENZEN

- ☐ Plugin installieren (z. B. "Limit Login Attempts Reloaded")
- ☐ Maximal drei Login-Versuche erlauben
- ☐ Sperre einstellen nach Fehlversuchen: 60 Minuten
- ☐ E-Mail-Benachrichtigung bei Sperren aktivieren

⚠️ **Wichtig:** Hacker probieren tausende Passwörter automatisch durch (sogenannte Brute-Force-Attacken). Nach drei Fehlversuchen ist Schluss. Aber: Begrenzte Login-Versuche sind kein ausreichender und dauerhafter Schutz. Immer zusätzliche Maßnahmen ergreifen!

SCHRITT 5: WORDPRESS UND PLUGINS AKTUELL HALTEN

- ☐ Automatische Updates aktivieren (WordPress-Kern)
- ☐ Plugins manuell oder automatisch aktualisieren
- ☐ Theme (Layout-Vorlage) aktuell halten
- ☐ E-Mail-Benachrichtigung bei verfügbaren Updates zusenden lassen

💡 **Tipp:** 60% der gehackten WordPress-Seiten hatten veraltete Plugins. Updates sind keine optionalen Maßnahmen sondern unerlässlich.

SCHRITT 6: UNGENUTZTE PLUGINS LÖSCHEN

- ☐ Liste aller installierten Plugins durchgehen
- ☐ Ungenutzte Plugins deaktivieren
- ☐ Deaktivierte Plugins löschen (nicht nur deaktivieren!)

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

🧩 **Beispiel:** Ein Kunde hatte 47 Plugins installiert. Genutzt hat er zwölf. Die anderen 35 waren nur Ballast und Risiko.

SCHRITT 7: SSL-VERSCHLÜSSELUNG AKTIVIEREN

- ☐ SSL-Zertifikat beim Hoster bestellen (oft kostenlos via Let's Encrypt)
- ☐ WordPress auf HTTPS umgestellen
- ☐ Weiterleitungen von HTTP auf HTTPS einrichten
- ☐ Grünes Schloss in der Browserzeile checken

📌 **Merke:** Ohne HTTPS werden Passwörter und Formulardaten unverschlüsselt übertragen. Google straft Seiten ohne HTTPS ab.

SCHRITT 8: DATENBANK-PRÄFIX ÄNDERN

- ☐ Nicht das Standard-Präfix "wp_" verwenden
- ☐ Eigenes Präfix setzen (z. B. "mf7_" oder "ac_")

⚠️ **Wichtig:** Hacker-Skripte zielen auf Standard-Tabellennamen wie „wp_users“. Anderes Präfix = Skript läuft ins Leere. Das Präfix können Sie nur bei der Installation setzen. Eine nachträgliche Änderung ist komplex – besser vom Profi machen lassen.

SCHRITT 9: FIREWALL INSTALLIEREN

- ☐ Sicherheitsoftware installieren (z. B. Wordfence, Sucuri, iThemes Security)
- ☐ Firewall aktivieren
- ☐ Malware Scan einrichten

- [ ] E-Mail-Benachrichtigung bei verdächtigen Aktivitäten aktivieren

💡 **Tipp:** Wordfence (kostenlos) blockt automatisch bekannte Angreifer-IPs und scannt Ihre Dateien nach Schadsoftware.

SCHRITT 10: REGELMÄSSIGE BACKUPS

- [ ] Plugin für Sicherheitskopien installieren (z. B. UpdraftPlus, BackWPup)
- [ ] Automatische Backups einrichten (mindestens wöchentlich)
- [ ] Externen Backup-Speicherort nutzen (Dropbox, Google Drive, eigener Server)
- [ ] Backup-Wiederherstellung testen

💡 **Tipp:** Sparen Sie nicht am falschen Ende. Wenn alles schiefgeht, ist ein Backup die Lebensversicherung für Ihre Website und Ihr Unternehmen.

ZUSÄTZLICHE SICHERHEITSTIPPS

- [ ] **Login-URL ändern**: Standard ist /wp-admin – ändern Sie das
- [ ] **Datei-Berechtigungen prüfen**: wp-config.php sollte 440 oder 400 haben, nicht 777
- [ ] **XML-RPC deaktivieren**: Wird oft für Angriffe missbraucht (über .htaccess-Datei)
- [ ] **Admin-Bereich per IP beschränken:** Nur Ihre IP darf auf Login zugreifen

DIE DREI HÄUFIGSTEN FEHLER

Fehler 1: "Mir passiert das nicht"
Falsch. Angriffe sind automatisiert. Jede Website ist ein potentielles Ziel.

Fehler 2: Sicherheit einmal machen, dann vergessen
Sicherheit ist ein Prozess, kein Zustand. Regelmäßig prüfen!

Fehler 3: Zu viele Sicherheitsplugins
1-2 gute Plugins reichen. Mehr bremsen die Website aus.

BONUS: WORAN SIE MERKEN, DASS SIE GEHACKT WURDEN

Warnsignale:

- Website lädt plötzlich langsam
- Unbekannte Admin-Konten tauchen auf
- Spam-Mails werden von Ihrer Domain verschickt
- Google warnt vor Ihrer Website ("Diese Seite könnte gehackt worden sein")
- Seltsame Dateien im FTP (z. B. mit Namen wie "x.php")

BONUS: WENN SIE GEHACKT WURDEN

1. Website sofort offline nehmen
2. Passwörter ändern (alle!)
3. Backup einspielen (von vor dem Hack)
4. Profi beauftragen für Bereinigung

🎯 **Sie möchten Ihre Website professionell absichern lassen?**
Ich übernehme das gerne für Sie.
→ kontakt@wildvariety.de