

WordPress-Sicherheits-Checkliste

20 Punkte, die Ihre WordPress-Website vor Hackern, Datenverlust und Ausfällen schützen. Prüfen Sie Ihre Seite jetzt.

 20 Sicherheitspunkte  5 Kategorien  Von Dennis Theis

1 Updates & Aktualisierungen

- ☐ **WordPress-Core auf dem neuesten Stand** Kritisch
Minor-Updates (z.B. 6.9.3 → 6.9.4) zeitnah einspielen, Major-Updates nach kurzem Test.
- ☐ **Alle Plugins aktuell** Kritisch
Veraltete Plugins sind Einfallstor Nr. 1. Wöchentlich prüfen.
- ☐ **Theme aktuell** Wichtig
Auch inaktive Themes können Sicherheitslücken enthalten — löschen oder updaten.
- ☐ **PHP-Version aktuell (mind. 8.2+)** Kritisch
Ältere PHP-Versionen erhalten keine Sicherheitspatches mehr.

TIPP

Aktivieren Sie automatische Minor-Updates in WordPress. Diese enthalten fast immer Sicherheitsfixes und sind abwärtskompatibel.

2 Zugänge & Passwörter

- ☐ **Starke Passwörter für alle Benutzer** Kritisch
Mindestens 16 Zeichen, Passwort-Manager empfohlen.
- ☐ **Zwei-Faktor-Authentifizierung (2FA) aktiv** Kritisch
Für alle Admin- und Editor-Konten. Plugin-Empfehlung: WP 2FA oder Wordfence.
- ☐ **Standard-Benutzername „admin“ geändert** Wichtig
Brute-Force-Angriffe zielen zuerst auf „admin“.
- ☐ **Login-Versuche begrenzt** Wichtig
Nach 5 fehlgeschlagenen Versuchen IP temporär sperren.
- ☐ **Ungenutzte Benutzerkonten entfernt** Empfohlen
Jedes Konto ist eine potenzielle Angriffsfläche.

TIPP

Nutzen Sie einen Passwort-Manager wie Bitwarden oder 1Password. Nie dasselbe Passwort für WordPress-Admin und E-Mail verwenden.

3 Backups & Wiederherstellung



- ☐ **Automatische Backups eingerichtet** Kritisch
Täglich für aktive Seiten, mindestens wöchentlich für alle anderen.
- ☐ **Backups extern gespeichert** Kritisch
Nicht nur auf demselben Server — Cloud-Speicher oder separater Server.
- ☐ **Wiederherstellung getestet** Wichtig
Ein Backup, das sich nicht wiederherstellen lässt, ist wertlos. Regelmäßig testen.

4 Sicherheitshärtung



- ☐ **SSL-Zertifikat aktiv (HTTPS)** Kritisch
Pflicht für DSGVO und Google-Ranking. Prüfen Sie das Schloss-Symbol im Browser.
- ☐ **Dateibearbeitung im Dashboard deaktiviert** Wichtig
DISALLOW_FILE_EDIT in wp-config.php setzen.
- ☐ **XML-RPC deaktiviert** Wichtig
Wird selten benötigt, ist aber ein häufiger Angriffsvektor.
- ☐ **Security Headers gesetzt** Wichtig
X-Content-Type-Options, X-Frame-Options, Content-Security-Policy konfigurieren.
- ☐ **WordPress-Versionnummer versteckt** Empfohlen
Gibt Angreifern weniger Informationen über Ihre Installation.

5 Monitoring & Pflege



- ☐ **Uptime-Monitoring aktiv** Wichtig
Sofortige Benachrichtigung bei Ausfällen — nicht erst wenn Kunden sich melden.
- ☐ **Malware-Scan regelmäßig** Kritisch
Automatischer Scan mindestens wöchentlich, bei kritischen Seiten täglich.
- ☐ **Ungenutzte Plugins und Themes entfernt** Wichtig
Deaktivieren reicht nicht — inaktive Plugins können trotzdem ausgenutzt werden.
- ☐ **Datenbank regelmäßig optimiert** Empfohlen
Revisionen, Spam-Kommentare und transiente Daten bereinigen.

Ihr Sicherheits-Score

Updates

___ / 4

Zugänge

___ / 5

Backups

___ / 3

Härtung

___ / 5

Monitoring

___ / 4

● 0–8: Dringend handeln

● 9–14: Verbesserungsbedarf

● 15–20: Gut geschützt

DEVSLAB

Keine Lust, das alles selbst zu machen?

Ich übernehme Ihre komplette WordPress-Wartung — alle Punkte dieser Checkliste und mehr. Ab 79€/Monat.

-  Persönlicher Ansprechpartner — kein Callcenter
-  Feste Reaktionszeiten mit SLA-Garantie
-  Updates, Backups, Sicherheit — alles inklusive
-  Premium-Plugin-Lizenzen ohne Aufpreis

Kostenlose Website-Analyse anfordern

✉ support@devslab.de ☎ +49 174 728 4457 🌐 devslab.de/wordpress-wartung