WordPress Sicherheits-Checkliste 2026

23 Punkte die jeder WordPress-Betreiber regelmäßig prüfen sollte – aktualisiert für 2026

Diese Checkliste hilft Ihnen, die Sicherheit Ihrer WordPress-Website Schritt für Schritt zu prüfen. Kein Fachvokabular, keine komplizierten Anleitungen – sondern klare, verständliche Hinweise für Website-Betreiber ohne technischen Hintergrund. Gehen Sie die Punkte idealerweise einmal im Monat durch.

Im Juli 2026 wurde eine der schwerwiegendsten WordPress-Sicherheitslücken der letzten Jahre bekannt: die sogenannte **WP2Shell-Angriffskette** (CVE-2026-63030 & CVE-2026-60137) ermöglicht es Hackern, ohne Benutzername oder Passwort die vollständige Kontrolle über eine WordPress-Website zu übernehmen. Innerhalb weniger Tage nach Bekanntwerden wurden Millionen von Angriffsversuchen registriert – vollautomatisch von Bots. Websites, die nicht sofort aktualisiert wurden, waren einem extrem hohen Risiko ausgesetzt. Das zeigt: Nur wer seine Website kontinuierlich wartet und Updates sofort einspielt, ist wirklich geschützt.

1. Updates & Aktualität

- [ ] **WordPress Core aktuell halten**
  Stellen Sie sich WordPress vor wie das Betriebssystem Ihres Computers – ohne Updates entstehen gefährliche Lücken. Prüfen Sie regelmäßig unter Dashboard → Aktualisierungen ob eine neuere Version verfügbar ist. Ein guter Turnus für reguläre Updates ist einmal im Monat. Bei bekannt gewordenen Sicherheitslücken gilt das aber nicht – dann müssen Patches kurzfristig, im besten Fall sofort, eingespielt werden. Im Juli 2026 wäre genau das bei der WP2Shell-Lücke entscheidend gewesen.

- [ ] **Alle Plugins aktualisieren**
  Ein Großteil aller WordPress-Sicherheitslücken steckt in Plugins. Nicht jedes veraltete Plugin ist gleich ein Sicherheitsrisiko, aber jedes Plugin kann potenziell Sicherheitslücken enthalten – das sollte regelmäßig überprüft werden. Auch hier gilt: einmal im Monat prüfen und aktualisieren ist ein guter Turnus – wird aber eine Sicherheitslücke in einem Ihrer Plugins bekannt, sollte das Update kurzfristig, im besten Fall sofort, eingespielt werden.

- [ ] **Alle Themes aktualisieren**
  Auch das Design Ihrer Website kann Sicherheitslücken enthalten – selbst wenn Sie das Theme gerade nicht aktiv nutzen. Themes die nicht gebraucht werden, sollten gelöscht statt nur deaktiviert werden. Reguläre Updates einmal im Monat reichen im Normalfall, bei bekannt gewordenen Sicherheitslücken sollte aber auch hier kurzfristig gepatcht werden.

- [ ] **PHP-Version aktuell**
  PHP ist die Programmiersprache hinter WordPress. Ältere PHP-Versionen erhalten keine Sicherheitsupdates mehr und sind ein beliebtes Angriffsziel. Empfohlen wird eine aktuelle PHP-Version – im Zweifel hilft Ihnen Ihr Hosting- oder Wartungsdienstleister gerne bei der Umstellung.

- [ ] **Inaktive Plugins & Themes löschen**
  Deaktivierte Plugins und Themes sind nicht sicher – sie können trotzdem angegriffen werden. Was Sie nicht brauchen, sollte vollständig gelöscht werden.

- [ ] **Unnötige Plugins & Themes vermeiden**
  Jedes zusätzliche Plugin ist potenziell eine weitere Schwachstelle. Fragen Sie sich bei jedem Plugin: Brauche ich das wirklich? Viele einfache Funktionen lassen sich mit wenig Aufwand auch direkt im eigenen Quellcode umsetzen, statt dafür ein ganzes Plugin zu installieren. Weniger ist hier mehr.

2. Backups – Ihre Lebensversicherung

- [ ] **Automatische Backups eingerichtet**
  Stellen Sie sich vor Ihre Website wird gehackt oder ein Update geht schief – ohne Backup wird es schwer, Ihre Website wieder in den vorherigen Zustand zu bringen. Richten Sie tägliche, automatische Backups ein. Verlassen Sie sich nicht auf manuelle Sicherungen.

- [ ] **Backups außerhalb des Servers speichern**
  Ein Backup das auf demselben Server wie Ihre Website liegt, hilft nicht wenn der Server ausfällt oder kompromittiert wird. Backups müssen auf einem externen Speicher – z. B. in der Cloud oder auf einem deutschen Server – gespeichert werden.

- [ ] **Backup-Wiederherstellung testen**
  Ein Backup ist nur so gut wie seine Wiederherstellung. Testen Sie mindestens einmal im Quartal ob Ihre Website aus dem Backup tatsächlich wiederhergestellt werden kann – bevor Sie es im Ernstfall wirklich brauchen.

- [ ] **Ausreichend Backup-Historie**
  Manchmal bemerkt man einen Hack erst Tage oder Wochen später. Dann hilft nur ein älteres Backup. Bewahren Sie mindestens 7–30 Tage Backup-Historie auf.

3. Zugänge & Passwörter

- [ ] **Starke Passwörter für alle Konten**
  Schwache Passwörter sind der häufigste Grund warum Websites gehackt werden. Verwenden Sie lange, zufällige Passwörter – am besten mit einem Passwort-Manager wie Bitwarden oder 1Password. Das gilt für WordPress, Hosting, FTP und Datenbank.

- [ ] **Zwei-Faktor-Authentifizierung (2FA) aktivieren**
  Selbst wenn jemand Ihr Passwort kennt, kann er sich ohne den zweiten Faktor (z. B. ein Code auf Ihrem Handy) nicht einloggen. 2FA ist eine der wirksamsten Schutzmaßnahmen überhaupt – und kostenlos einzurichten.

- [ ] **Benutzernamen "admin" nicht verwenden**
  Der Benutzername "admin" ist das Erste was Hacker ausprobieren. Verwenden Sie stattdessen einen individuellen Benutzernamen der nichts mit Ihrem Namen oder Ihrer Website zu tun hat.

- [ ] **Veraltete Benutzerkonten löschen**
  Hat eine frühere Agentur oder ein ehemaliger Mitarbeiter noch Zugang zu Ihrer Website? Prüfen Sie regelmäßig alle Benutzerkonten und löschen Sie alles was nicht mehr benötigt wird. Nach der WP2Shell-Lücke empfahlen Sicherheitsforscher besonders, unbekannte Admin-Konten zu entfernen.

4. Monitoring & Überwachung

- [ ] **Uptime-Monitoring einrichten**
  Wissen Sie sofort wenn Ihre Website offline geht? Ohne Monitoring erfahren Sie es erst wenn ein Kunde Sie anruft. Mit einem Uptime-Monitor werden Sie automatisch benachrichtigt – oft bevor Ihre Besucher es bemerken.

- [ ] **Sicherheitslücken in Plugins überwachen**
  Regelmäßig werden neue Sicherheitslücken in WordPress-Plugins entdeckt, die teils sehr schnell aktiv ausgenutzt werden. Dienste wie Patchstack überwachen Ihre Plugins und warnen Sie automatisch.

- [ ] **SSL-Zertifikat prüfen**
  Das Schloss-Symbol in der Browser-Leiste zeigt an dass Ihre Website verschlüsselt überträgt. Dieses Zertifikat läuft regelmäßig ab und muss erneuert werden. Prüfen Sie das Ablaufdatum mindestens einmal im Quartal.

5. Technische Absicherung

- [ ] **Login-Bereich schützen**
  Die Standard-Adresse /wp-admin/ ist bei Hackern bestens bekannt. Sichern Sie den Login-Bereich zusätzlich ab – z. B. durch einen extra Passwortschutz oder indem Sie die Adresse umbenennen.

- [ ] **XML-RPC deaktivieren**
  XML-RPC ist eine versteckte Schnittstelle in WordPress die von außen erreichbar ist – und die die meisten Websites gar nicht brauchen. Deaktivieren Sie sie, um eine häufig genutzte Hintertür zu schließen.

- [ ] **Datei-Berechtigungen korrekt setzen**
  Dateien auf Ihrem Server sollten nur die Rechte haben die sie wirklich brauchen. Zu offene Berechtigungen ermöglichen es Angreifern, Dateien zu verändern. Fragen Sie Ihren Hoster oder Wartungsdienstleister ob die Berechtigungen korrekt gesetzt sind.

- [ ] **Firewall & Brute-Force-Schutz einrichten**
  Eine WordPress-Firewall erkennt automatisch verdächtige Anfragen und blockiert Angriffe bevor sie Schaden anrichten können. Brute-Force-Schutz verhindert dass Bots tausende Passwörter durchprobieren. Wichtig: Ein Sicherheits-Plugin allein reicht nicht – es muss nach der Installation sorgfältig konfiguriert werden, sonst bietet es kaum Schutz.

- [ ] **Alle WordPress-Installationen auf dem Webspace schützen**
  Haben Sie mehrere WordPress-Installationen auf demselben Webspace, z. B. für verschiedene Projekte oder Subdomains? Dann reicht es nicht, nur eine davon abzusichern. Wird eine Installation gehackt, können Angreifer darüber oft auch auf die anderen zugreifen – selbst wenn diese eigentlich gut geschützt sind. Achten Sie deshalb darauf, dass wirklich jede WordPress-Installation auf Ihrem Webspace aktuell gehalten und abgesichert ist.

- [ ] **Sicherheits-Header setzen**
  Neben WordPress selbst lässt sich auch auf Server-Ebene zusätzlicher Schutz einrichten – über sogenannte Sicherheits-Header wie HSTS oder X-Frame-Options. Sie sorgen z. B. dafür, dass Ihre Website nur verschlüsselt aufgerufen werden kann und nicht unbemerkt in fremde Seiten eingebettet wird. Die Einrichtung ist technischer als die anderen Punkte – fragen Sie im Zweifel Ihren Hosting- oder Wartungsdienstleister danach.

Hinweis: Diese Checkliste erhebt keinen Anspruch auf Vollständigkeit und ersetzt keine individuelle fachliche Beratung. WordPress-Sicherheit ist ein fortlaufendes Thema – je nach Website, Plugins und Einsatzzweck können weitere Maßnahmen sinnvoll sein. Sind Sie sich unsicher oder haben den Verdacht, dass Ihre Website bereits kompromittiert ist, lassen Sie sich in jedem Fall von einem Profi beraten.