

DNKLD SGN

branding/marketing/webdesign

WordPress- Wartungs- & Sicherheitscheckliste

Praktische Checkliste für einen stabilen und gepflegten Website-Betrieb



WordPress-Wartungs- & Sicherheitscheckliste

Eine WordPress-Website bleibt nur zuverlässig, wenn Updates, Backups, Sicherheit, Monitoring und Funktionstests regelmäßig durchgeführt werden. Diese Checkliste unterstützt einen strukturierten Wartungsprozess.

So nutzen Sie die Checkliste

Prüfen Sie jeden Punkt aus Sicht Ihrer Kunden. Markieren Sie offene Punkte und priorisieren Sie anschließend die Maßnahmen, die Vertrauen, Verständlichkeit, Bedienbarkeit oder Anfragen am stärksten beeinflussen.

01 Verantwortung und Zugänge

- ☐ Domain, Hosting, WordPress, E-Mail und externe Dienste sind dem Unternehmen eindeutig zugeordnet.
- ☐ Administrator-Zugänge werden nur an Personen vergeben, die sie tatsächlich benötigen.
- ☐ Jede Person nutzt einen eigenen Benutzer statt gemeinsam verwendeter Konten.
- ☐ Zugänge ausscheidender Mitarbeiter oder Dienstleister werden zeitnah entfernt.
- ☐ Passwörter werden sicher verwaltet und nicht unverschlüsselt per E-Mail verteilt.
- ☐ Für Notfälle ist dokumentiert, wer Hosting, Domain und Backups erreichen kann.

02 Backups und Wiederherstellung

- ☐ Datenbank und WordPress-Dateien werden regelmäßig vollständig gesichert.
- ☐ Backup-Häufigkeit passt zur Änderungsfrequenz der Website.
- ☐ Mindestens eine Sicherung liegt getrennt vom Webserver.
- ☐ Backups werden automatisch überwacht und Fehler gemeldet.
- ☐ Vor größeren Updates oder Änderungen wird eine zusätzliche Sicherung erstellt.
- ☐ Die Wiederherstellung wurde praktisch getestet und nicht nur theoretisch vorausgesetzt.

03 Updates und Testumgebung

- ☐ WordPress-Core, Plugins und Themes werden zeitnah aktualisiert.
- ☐ Vor Updates werden Changelogs, Kompatibilität und bekannte Probleme geprüft.
- ☐ Kritische Änderungen werden zuerst in einer Staging- oder Testumgebung geprüft.
- ☐ Nach Updates werden Startseite, Navigation, Formulare, Suche und zentrale Funktionen getestet.
- ☐ Nicht mehr unterstützte PHP-, WordPress- oder Plugin-Versionen werden ersetzt.
- ☐ Automatische Updates sind bewusst konfiguriert und werden kontrolliert.

04 Plugins und Themes

- ☐ Installiert sind nur Plugins und Themes, die tatsächlich benötigt werden.
- ☐ Unbenutzte Plugins und Themes werden gelöscht statt nur deaktiviert.
- ☐ Erweiterungen stammen aus vertrauenswürdigen Quellen und werden aktiv gepflegt.
- ☐ Doppelte Funktionen durch mehrere Plugins werden vermieden.

- ☐ Lizenzen, Verlängerungen und Update-Zugänge sind dokumentiert.
- ☐ Ein Child Theme oder eine updatefeste Lösung schützt individuelle Anpassungen.

05 Anmeldung und Benutzerkonten

- ☐ Starke, einzigartige Passwörter sind für alle privilegierten Konten verpflichtend.
- ☐ Zwei-Faktor-Authentifizierung ist mindestens für Administratoren aktiviert.
- ☐ Anmeldeversuche und auffällige Aktivitäten werden begrenzt oder überwacht.
- ☐ Benutzerrollen vergeben nur die tatsächlich benötigten Rechte.
- ☐ Standard- oder leicht erratbare Benutzernamen werden vermieden.
- ☐ Kontowiederherstellung und Notfallzugriff sind sicher organisiert.

06 Technische Absicherung

- ☐ Die Website ist vollständig über HTTPS erreichbar und leitet HTTP korrekt weiter.
- ☐ Datei- und Verzeichnisrechte sind angemessen gesetzt.
- ☐ Sensible Konfigurationsdateien und Verzeichnisse sind vor öffentlichem Zugriff geschützt.
- ☐ Fehlermeldungen geben Besuchern keine internen Server- oder Datenbankdetails preis.
- ☐ Sicherheitsheader und Serverkonfiguration werden durch fachkundige Personen geprüft.
- ☐ Änderungen an Server, Datenbank oder Konfiguration erfolgen nur mit aktuellem Backup.

07 Performance und Datenbank

- ☐ Bilder werden in geeigneten Abmessungen und modernen Formaten ausgeliefert.
- ☐ Caching ist passend zu Hosting und Website eingerichtet.
- ☐ Unnötige Skripte, externe Fonts und Drittanbieter-Dienste wurden reduziert.
- ☐ Datenbanktabellen, Revisionen und temporäre Daten werden kontrolliert gepflegt.
- ☐ Cronjobs und Hintergrundprozesse laufen zuverlässig.
- ☐ Performance wird mit realistischen Seiten und Geräten statt nur auf der Startseite geprüft.

08 Monitoring und Fehlerkontrolle

- ☐ Ein Uptime-Monitor meldet Ausfälle zeitnah.
- ☐ Server-, PHP- und WordPress-Fehlerprotokolle werden regelmäßig kontrolliert.
- ☐ Sicherheitswarnungen und ungewöhnliche Dateiänderungen werden überwacht.
- ☐ SSL-Zertifikat, Domain und wichtige Lizenzen besitzen rechtzeitige Ablaufwarnungen.
- ☐ Defekte Links und 404-Fehler werden wiederkehrend ausgewertet.
- ☐ Kontaktformulare und E-Mail-Zustellung werden mit echten Tests überprüft.

09 Datenschutz und externe Dienste

- ☐ Alle eingebundenen Analyse-, Marketing-, Karten-, Video- und Schriftendienste sind dokumentiert.
- ☐ Einwilligungen werden technisch passend zum tatsächlichen Einsatz gesteuert.
- ☐ Datenschutzerklärung und Anbieterangaben werden bei Änderungen aktualisiert.
- ☐ Formulardaten werden nur so lange gespeichert, wie es erforderlich und vorgesehen ist.
- ☐ Zugriff auf personenbezogene Daten ist auf notwendige Personen begrenzt.

- ☐ Externe Dienste werden regelmäßig auf Notwendigkeit, Kosten und Datenschutz geprüft.

10 Wartungsrhythmus und Dokumentation

- ☐ Es gibt einen festen monatlichen Termin für Updates, Backups und Funktionstests.
- ☐ Quartalsweise werden Performance, Benutzer, Plugins, Inhalte und Conversion-Wege geprüft.
- ☐ Mindestens jährlich werden Hosting, PHP-Version, Sicherheitskonzept und Notfallplan bewertet.
- ☐ Änderungen, Störungen und Wiederherstellungen werden nachvollziehbar dokumentiert.
- ☐ Verantwortlichkeiten zwischen Unternehmen, Hoster und Dienstleister sind schriftlich geklärt.
- ☐ Für kritische Störungen existiert ein realistischer Eskalations- und Kommunikationsplan.

Ihre Auswertung

Wählen Sie die drei Maßnahmen mit dem größten Hebel. Formulieren Sie jeweils eine konkrete Aufgabe, eine verantwortliche Person und einen realistischen Termin.

1. Priorität

2. Priorität

3. Priorität

Backups sind erst nach einem Test verlässlich

Eine vorhandene Sicherungsdatei ist noch kein Notfallplan. Entscheidend ist, dass Zuständigkeiten, Zugang und Wiederherstellung unter realistischen Bedingungen funktionieren.

Sicherheitshinweis: Diese Checkliste ersetzt kein professionelles Sicherheits-Audit. Server- und Konfigurationsänderungen sollten nur durch qualifizierte Personen und mit aktuellem Backup erfolgen.

Orientierung und weiterführende Quellen

WordPress Developer Handbook: Hardening WordPress

WordPress Developer Handbook: Backups

WordPress Developer Handbook: Monitoring