Technische Wartung von WordPress

Tipps aus der Praxis: Updates, Fehlerbehebung, Sicherheit, Backups und Performance

1. Vor jedem Update

- **Backup erstellen.** Sichern Sie vor jeder Aktualisierung immer **Dateien und Datenbank**. Ein Backup nur der Dateien reicht nicht, denn Inhalte und Einstellungen liegen in der Datenbank.
- **Testumgebung nutzen.** Bei Installationen mit vielen Plugins sollten Sie Aktualisierungen zuerst auf einer Testumgebung (Staging) durchführen. Manchmal entstehen Konflikte, und Ihre Seite funktioniert danach nicht mehr. Viele Hoster bieten Staging mit einem Klick an.
- **Changelogs lesen.** Achten Sie besonders auf große Versionssprünge (z. B. von 3.x auf 4.0). Sie bringen häufiger tiefgreifende Änderungen oder neue Mindestanforderungen mit.
- **Kompatibilität prüfen.** Stimmen die Angaben zur WordPress- und PHP-Version mit Ihrer Installation überein?
- **Ruhige Zeiten wählen.** Aktualisieren Sie nicht kurz vor dem Feierabend oder Wochenende und nicht zu Stoßzeiten (z. B. im Onlineshop).

2. Beim Aktualisieren

- **Sinnvolle Reihenfolge einhalten:** zuerst WordPress selbst, danach die Plugins, dann die Themes und zum Schluss die Übersetzungen.
- **Einzeln statt alle auf einmal.** Bei vielen Aktualisierungen hilft es, die Plugins nacheinander zu aktualisieren und nach zwei oder drei Updates die Plugin-Seite neu zu laden. So erkennen Sie sofort, welches Update ein Problem verursacht hat.
- **Premium-Plugins nicht vergessen.** Kostenpflichtige Plugins aktualisieren sich oft nur mit gültigem Lizenzschlüssel. Prüfen Sie, ob Ihre Lizenzen noch aktiv sind.
- **Child-Theme verwenden.** Eigene Anpassungen am Theme gehören in ein Child-Theme. Sonst überschreibt das nächste Theme-Update Ihre Änderungen.

3. Nach dem Update

- **Einstellungen prüfen.** Kontrollieren Sie nach einem Plugin-Update immer die Einstellungen, die Sie vorgenommen haben. Bei manchen Plugins werden sie zurückgesetzt.
- **Cache leeren:** im Caching-Plugin, beim Hoster, im CDN und im eigenen Browser.
- **Wichtige Funktionen testen:** Startseite, Menü, Kontaktformulare (kommt die E-Mail wirklich an?), Suche, Login, im Shop auch Warenkorb und Checkout. Schauen Sie sich die Seite auch auf dem Smartphone an.
- **Fehlerlog ansehen.** Neue Warnungen weisen oft schon auf ein Problem hin, bevor Besucher es bemerken.

4. Wenn nach einem Update etwas nicht mehr funktioniert

- **Plugin per FTP deaktivieren.** Wenn Sie nach einem Update eine Fehlermeldung bekommen, können Sie Plugins auch über FTP deaktivieren. Löschen müssen Sie das Plugin nicht. Es reicht, im Ordner `/wp-content/plugins/` dem Plugin-Ordner einen Unterstrich voranzustellen (z. B. `_kontaktformular`). Dann deaktiviert WordPress das Plugin, und Sie können Ihr Backend wieder nutzen. Danach entfernen Sie den Unterstrich wieder und aktivieren das Plugin im Backend erst, wenn das Problem gelöst ist.
- **Unklar, welches Plugin schuld ist?** Benennen Sie den ganzen Ordner `plugins` um (z. B. in `plugins_alt`). Damit sind alle Plugins deaktiviert. Benennen Sie ihn danach zurück und aktivieren Sie die Plugins im Backend einzeln wieder.
- **Theme als Ursache prüfen.** Benennen Sie den Ordner des aktiven Themes um. WordPress wechselt dann auf ein installiertes Standard-Theme (z. B. „Twenty Twenty-Five“). Löschen Sie deshalb immer mindestens ein Standard-Theme nicht.
- **E-Mail zum Wiederherstellungsmodus.** Bei schweren Fehlern schickt WordPress eine E-Mail mit einem Link zum Wiederherstellungsmodus an die Admin-Adresse. Über diesen Link können Sie sich trotz Fehler anmelden und das betroffene Plugin deaktivieren. Deshalb sollte die Admin-E-Mail-Adresse aktuell sein.
- **Fehlermeldungen sichtbar machen.** Tragen Sie in der `wp-config.php` Folgendes ein. Die Fehler werden dann in `/wp-content/debug.log` gespeichert und nicht öffentlich angezeigt. Schalten Sie das nach der Fehlersuche wieder ab.

```
define( 'WP_DEBUG', true );
define( 'WP_DEBUG_LOG', true );
define( 'WP_DEBUG_DISPLAY', false );
```

- **Seite hängt im Wartungsmodus.** Erscheint dauerhaft „Kurzzeitig nicht verfügbar wegen Wartungsarbeiten“, löschen Sie die Datei `.maintenance` im Hauptverzeichnis der Installation.
- **Speicherlimit erhöhen.** Bei „Allowed memory size exhausted“ hilft `define( 'WP_MEMORY_LIMIT', '256M' );` in der `wp-config.php`, sofern Ihr Hoster das zulässt.
- **404-Fehler auf Unterseiten.** Öffnen Sie *Einstellungen → Permalinks* und klicken Sie einmal auf „Speichern“. Dadurch wird die `.htaccess` neu geschrieben.
- **Alte Version zurückspielen.** Ist ein Update fehlerhaft, können Sie auf die Vorversion zurückgehen, über Ihr Backup oder ein Rollback-Plugin. Melden Sie den Fehler dem Entwickler.

5. Sicherheit

- **Nicht genutzte Plugins und Themes löschen.** Auch deaktivierte Plugins können Sicherheitslücken enthalten.
- **Nur aus seriösen Quellen installieren:** aus dem offiziellen WordPress-Verzeichnis oder direkt beim Hersteller. Finger weg von „nulled“ (gecrackten) Premium-Plugins, denn sie enthalten häufig Schadcode.
- **Plugins ohne Pflege ersetzen.** Ein Plugin, das seit Jahren nicht aktualisiert wurde, sollten Sie gegen eine gepflegte Alternative tauschen.
- **Sichere Anmeldung:** starke, einmalige Passwörter, Zwei-Faktor-Authentifizierung, kein Benutzername „admin“ und eine Begrenzung der Login-Versuche.
- **Benutzerrollen sparsam vergeben.** Nicht jeder braucht Administratorrechte. Entfernen Sie Konten von ehemaligen Mitarbeitern und Dienstleistern.
- **Dateieditor im Backend abschalten:** `define( 'DISALLOW_FILE_EDIT', true );`
- **Dateirechte prüfen.** Üblich sind 755 für Ordner und 644 für Dateien. Die `wp-config.php` sollte noch restriktiver sein (z. B. 440 oder 400).
- **SSL/HTTPS** für die gesamte Seite aktivieren und das Zertifikat automatisch verlängern lassen.
- **Sicherheitsschlüssel erneuern.** Nach einem Verdacht auf einen Angriff tauschen Sie die Salts in der `wp-config.php` aus. Danach werden alle Benutzer abgemeldet.

6. Backups richtig machen

- **Automatisch und regelmäßig sichern.** Wie oft, hängt davon ab, wie häufig sich die Inhalte ändern. Bei Shops ist eine tägliche Sicherung sinnvoll.
- **Backups extern lagern**, also nicht nur auf demselben Server. Bewährt hat sich die 3-2-1-Regel: drei Kopien auf zwei verschiedenen Medien, davon eine an einem anderen Ort.
- **Wiederherstellung testen.** Ein Backup, das sich nicht zurückspielen lässt, nützt im Ernstfall nichts.

7. Performance und Datenbank

- **Caching** einsetzen, über ein Plugin oder serverseitig beim Hoster.
- **Bilder optimieren:** vor dem Hochladen verkleinern, moderne Formate wie WebP verwenden und Lazy Loading nutzen.
- **Datenbank aufräumen:** alte Beitragsrevisionen, Spam- und Papierkorb-Kommentare, abgelaufene Transients und Reste gelöschter Plugins entfernen. Machen Sie vorher ein Backup. Die Zahl der gespeicherten Revisionen lässt sich begrenzen:

```
define( 'WP_POST_REVISIONS', 5 );
```

- **WP-Cron ersetzen.** Bei Seiten mit wenig oder sehr viel Besucherverkehr kann es sinnvoll sein, WP-Cron abzuschalten (`define( 'DISABLE_WP_CRON', true );`) und stattdessen einen echten Cronjob beim Hoster einzurichten.
- **Ladezeit regelmäßig messen**, z. B. mit Google PageSpeed Insights.

8. Server und PHP

- **PHP-Version aktuell halten.** Veraltete PHP-Versionen bekommen keine Sicherheitsupdates mehr und sind langsamer. Testen Sie einen Wechsel vorher auf der Testumgebung.
- **Website-Zustand prüfen.** Unter *Werkzeuge* → *Website-Zustand* zeigt WordPress selbst Probleme und Empfehlungen an.
- **Speicherplatz und Datenbankgröße im Blick behalten.** Ist der Webspace voll, schlagen Updates und Backups fehl.

9. Überwachung

- **Erreichbarkeit überwachen** mit einem Uptime-Monitor, der Sie bei einem Ausfall sofort per E-Mail oder App benachrichtigt.
- **Google Search Console** auf Crawling-Fehler, Sicherheitswarnungen und Indexierungsprobleme prüfen.
- **Defekte Links** regelmäßig suchen und reparieren.
- **Formulare und den E-Mail-Versand testen.** Für zuverlässige Zustellung ist ein SMTP-Plugin oft besser als der Standardversand von PHP.

10. Wartungsrhythmus (Checkliste)

Wann	Was
Wöchentlich	Updates prüfen und einspielen, Backups kontrollieren, Formulare testen
Monatlich	Datenbank aufräumen, Fehlerlogs und Website-Zustand prüfen, Ladezeit messen, Spam entfernen
Vierteljährlich	Wiederherstellung eines Backups testen, Benutzerkonten und Rechte prüfen, ungenutzte Plugins und Themes löschen, PHP-Version und Lizenzen kontrollieren
Jährlich	Plugin-Bestand insgesamt überprüfen (Gibt es bessere oder schlankere Alternativen?), Datenschutzerklärung und Impressum auf Aktualität prüfen