WordPress-Plugins & Sicherheit – Checkliste

Plugin-Auswahl und laufende Kontrolle ohne Scheinsicherheit.

PRÜFPUNKTE FÜR EIN PLUGIN

Bevor ein Plugin bleibt: Pflege, Anbieter und Risiko prüfen.

- [ ] Das letzte Update liegt nicht lange zurück, und das Plugin ist mit der aktuellen WordPress- und PHP-Version getestet
- [ ] Der Änderungsverlauf zeigt regelmäßige Pflege, auch bei Sicherheitskorrekturen
- [ ] Der Anbieter ist identifizierbar und erreichbar, mit Impressum, Support und Dokumentation
- [ ] Es gibt eine nachvollziehbare Nutzerbasis und Rückmeldungen, auch zu Support-Fragen
- [ ] Die Bezugsquelle ist das offizielle Verzeichnis oder die Website des Anbieters, nicht eine „kostenlose“ Kopie eines Premium-Plugins
- [ ] Der Funktionsumfang passt zum Bedarf; das Plugin bringt keine großen Zusatzfunktionen mit, die nicht gebraucht werden
- [ ] Das Plugin verarbeitet keine sensiblen Daten, oder der Anbieter erklärt nachvollziehbar, wie er damit umgeht

Plugin-Inventar – Mindestangaben

Angabe	Warum sie wichtig ist
Name, Version, Anbieter	Sicherheitsmeldungen zuordnen
Zweck auf der Website	Bedarf und Ausfallrisiko erkennen
Bezugsquelle	Update-Weg bestimmen
Datum des letzten Updates	Signal für aufgegebene Plugins
Risikoklasse	Formulare, Uploads, Zahlungen priorisieren

KOMPAKTE CHECKLISTE FÜR DEN BETRIEB

Inventar, Updates und Austauschplan für den Betrieb.

- [ ] Es gibt ein Plugin-Inventar mit Zweck, Bezugsquelle, Version, Update-Datum und Lizenz
- [ ] Ungenutzte und deaktivierte Plugins sind vollständig entfernt
- [ ] Aufgegebene Plugins sind identifiziert und haben einen Austauschplan
- [ ] Neue Plugins werden vor der Installation anhand fester Kriterien geprüft
- [ ] Sicherheitsupdates werden zeitnah eingespielt, nicht erst im nächsten regulären Termin
- [ ] Vor dem Update liegt ein Backup, danach folgt ein Test der wichtigen Funktionen
- [ ] Lizenzen für Premium-Plugins sind auf das Unternehmen registriert, Ablaufdaten sind notiert
- [ ] Jemand beobachtet Sicherheitsmeldungen zu den eingesetzten Plugins
- [ ] Ein Plan beschreibt, was bei einer Lücke ohne Patch geschieht
- [ ] Zugänge sind einzeln vergeben und mit Zwei-Faktor-Anmeldung geschützt