WordPress-Sicherheits-Checkliste

Für Schweizer KMU. Praktisch, in einer halben Stunde umsetzbar.

> Du betreibst eine WordPress-Webseite und willst wissen, wo du stehst.
> Diese Liste führt dich durch die wichtigsten Prüfpunkte in drei Stufen:
> Sofort prüfen (heute) → Monatlich tun → Einmal richtig einrichten.

// 01

Sofort prüfen

Heute, 15-30 Min

- [ ] 01 WordPress-Core ist auf der neuesten Version.
  Admin → Dashboard → Aktualisierungen. Alle Updates einspielen.
- [ ] 02 Alle aktiven Plugins sind aktuell.
  Auch die unscheinbaren. Sortiere nach 'Update verfügbar'.
- [ ] 03 Inaktive oder ungenutzte Plugins entfernt.
  Deaktivieren reicht nicht. Löschen, sonst bleibt der Code angreifbar.
- [ ] 04 Kein Plugin ist seit über 6 Monaten ohne Update.
  Verlassene Plugins sind die häufigste Hack-Ursache.
- [ ] 05 Admin-Passwort ist 16+ Zeichen lang, mit 2FA.
  Plugin: 'Two Factor Authentication' oder 'WP 2FA'.
- [ ] 06 Letztes Backup ist nicht älter als 7 Tage.
  Und es liegt nicht auf dem gleichen Server wie die Webseite.

// 02

Monatlich tun

Ca. 30 Min/Monat

- [ ] 07 Plugin-Updates manuell durchgehen, nicht blind auto-update.
  Auto-Update kann eine kompatible Konfiguration brechen.
- [ ] 08 Login-Logs auf ungewöhnliche Versuche prüfen.
  Plugin: 'Wordfence' oder 'WPS Hide Login' liefert die Logs.
- [ ] 09 SSL-Zertifikat ist gültig und erneuert sich automatisch.
  Let's Encrypt: Cron-Job läuft? Kein Ablauf in 30 Tagen?
- [ ] 10 Backup-Wiederherstellungs-Test durchgeführt.
  Theoretisch ein Backup zu haben reicht nicht. Probiere es aus.

// 03

Einmal richtig einrichten

1-2 Stunden, dann erledigt

- [ ] **11** Web Application Firewall ist aktiv (Cloudflare oder Wordfence).
  Filtert die häufigsten Angriffsmuster bevor sie WordPress erreichen.
- [ ] **12** Rate-Limit oder Fail2Ban für /wp-login.php konfiguriert.
  Stoppt Brute-Force-Versuche nach wenigen Fehlversuchen.
- [ ] **13** wp-config.php hat Berechtigung 640 oder restriktiver.
  chmod 640 wp-config.php. Standard 644 ist zu offen.
- [ ] **14** File-Editing im Admin deaktiviert.
  In wp-config.php: define('DISALLOW_FILE_EDIT', true);
- [ ] **15** XML-RPC deaktiviert, wenn nicht benötigt.
  Häufiger Angriffsvektor für Brute-Force und DDoS.

// 04

Wann eine Migration ernsthaft prüfen

Entscheidung in 5 Min

- → Deine Webseite ist primär eine Visitenkarte, kein interaktives System.
- → Du planst neue Funktionen wie ein Kundenportal oder Mandanten-Login.
- → Mehr als die Hälfte deiner Wartungszeit geht in Sicherheits-Patches.
- → Du hattest bereits einen Hack oder Beinahe-Vorfall.
- → Deine Webseite ist über 5 Jahre alt und nie strukturell überarbeitet.

// 05

Wenn es bereits passiert ist

Sofort handeln

72 Stunden Meldepflicht.
Art. 24 revDSG verlangt Meldung an EDÖB bei Datenpannen innert 72 Std.

BACS-Meldeformular nutzen.
ncsc.admin.ch/Meldeformular. Auch bei nicht meldepflichtigen Vorfällen sinnvoll.

Keine alten Backups blind einspielen.
Der Angriff begann oft Tage vorher. Backups könnten bereits infiziert sein.

Experten holen, nicht selbst herumdoktern.
Forensik vor Bereinigung. Sonst kommt der Angreifer beim nächsten Bug wieder.

// FRAGEN ODER MIGRATION?

Ehrliche Architektur-Beratung, 30 Min, kostenlos.

Auch wenn die Antwort lautet: bleib bei WordPress, aber repariere folgende Dinge.