

WordPress-Sicherheit: in der richtigen Reihenfolge

Arbeite zuerst Stufe 1 vollständig ab, dann Stufe 2. Was keine Priorität hat, ersetzt keine Stufe. Diese Maßnahmen müssen auch nach der Einrichtung gepflegt werden. Für den Ernstfall steht der Notfallplan am Ende.

STUFE 1 · ZUERST: GROSSE WIRKUNG, WENIG AUFWAND

- | | |
|---|--|
| ☐ WordPress-Kern aktuell , automatische Updates nicht abgeschaltet | ☐ Alle Plugins und das Theme aktuell , Updates in festem Rhythmus |
| ☐ Ungenutzte Plugins und Themes gelöscht , nicht nur deaktiviert | ☐ Jedes Plugin geprüft : letztes Update, getestet bis, Support, Herkunft |
| ☐ Lange, einmalige Passwörter für WordPress, Hosting, FTP und Datenbank | ☐ Zwei-Faktor-Anmeldung für alle Admins |
| ☐ Kein Benutzer „admin“ oder „webmaster“ | ☐ Backups außerhalb des Servers , mehrere Stände, Wiederherstellung getestet |

Wenn du deine Zugänge nicht kennst: Klär zuerst, wer Hosting, Domain, Administratorzugänge und Plugin-Lizenzen besitzt, wer Warnungen erhält und wer Backups wiederherstellen kann.

STUFE 2 · DANACH: SOLIDE HÄRTUNG, ETWAS TECHNIK

- | | |
|--|--|
| ☐ Admin-Rechte nur, wo nötig , sonst Rolle Redakteur oder Autor | ☐ Alte Konten gelöscht , etwa früherer Mitarbeitender oder Dienstleister |
| ☐ Dateieditor abgeschaltet : DISALLOW_FILE_EDIT in der wp-config.php | ☐ Dateirechte eng : schreibbar im Wesentlichen nur /wp-content/ |
| ☐ wp-config.php nur für dich und den Webserver lesbar | ☐ Login-Versuche begrenzt , beim Hoster oder per Plugin |
| ☐ XML-RPC geschützt oder abgeschaltet , wenn nicht gebraucht | ☐ SFTP statt FTP für die Verbindung zum Server |
| ☐ Server und PHP aktuell , keine PHP-Version ohne Sicherheitsupdates | |

Keine Priorität, kein Ersatz für Schutz: Login-URL verstecken, Tabellenpräfix ändern, ein zweites Sicherheits-Plugin. Wenn überhaupt, erst wenn Stufe 1 und 2 stehen.

NOTFALLPLAN: WORDPRESS GEHACKT

Schritt	Was du tust	Erledigt
1 · Dokumentieren	Was du siehst, seit wann, was sich zuletzt geändert hat	☐
2 · Hoster informieren, scannen	Hoster einbeziehen, Website und eigenen Rechner auf Schadsoftware prüfen	☐
3 · Zugänge zurücksetzen	Alle Passwörter und neue Sicherheitsschlüssel	☐
4 · Befallenen Stand sichern	Kopie von Dateien und Datenbank vor dem Aufräumen	☐
5 · Bereinigen	Sauberes Backup zurückspielen oder Kern neu aufspielen und prüfen	☐
6 · Aktualisieren	Alles aktuell, Passwörter ein zweites Mal ändern	☐
7 · Ursache finden	Lücke schließen, danach Stufe 1 und 2 abarbeiten	☐

Personenbezogene Daten betroffen? Nach Art. 33 DSGVO kann eine Meldung an die Aufsichtsbehörde nötig sein, möglichst binnen 72 Stunden, bei hohem Risiko nach Art. 34 auch an die Betroffenen. Jeden Vorfall intern dokumentieren. Zieh früh deine Datenschutzberatung hinzu. Diese Checkliste ist keine Rechtsberatung.

Du willst Updates und Backups nicht selbst im Blick behalten?

Schreib mir, wer deine WordPress-Website heute betreut. Ich sage dir, welche Maßnahmen bei dir zuerst kommen.

hallo@inventivo.de