

Die Mauer: Sicherheits Web-Check

Ein Hack schadet massiv deiner Marken-Reputation, kostet wochenlange Google Rankings und vernichtet Kundendaten. Schließe die Basis-Sicherheitslücken in WordPress ab Sekunde 1 konsequent.

1. Das Einfallstor (WordPress Login)

- Admin Account ist NICHT "Admin":** Den Username "admin" zu benutzen, spart Hackern 50% der Brute-force-Arbeit. Hast du einen alternativen Benutzernamen?
- Login-Pfad obfuskiert:** Die URL /wp-admin wurde dauerhaft versteckt (z.B. mit einem Tool wie WPS Hide Login) und verweist nun auf etwas Kryptisches (z.B. /zugang-rwg).
- Zwei-Faktor-Authentifizierung (2FA):** Ist für Administratoren zwingend eine Code-App (Google Authenticator) bei jedem Login hinterlegt?
- Brute-Force Sperre:** Nach 3 bis 5 falschen Passworteingaben wird die betreffende IP für mindestens 24 Stunden global gesperrt.

2. Serverseitige Abschottung & Updates

- Web Application Firewall (WAF):** Gibt es eine Firewall, die böswillige Bots und SQL-Zusätze im Datenverkehr blockt (via Cloudflare, Wordfence oder Limit Login Attempts)?
- Datenbank Präfix:** Das WordPress-Datenbank Präfix heißt beim Setup niemals standardmäßig wp_, sondern kryptisch (z.B. wpx_9n2_).
- Keine ungenutzten Erweiterungen:** Plugins und Themes, die inaktiviert rumliegen, dienen als Hintertüren. Radikale Maßnahme: Komplette löschen, nicht nur abstellen.
- PHP Version up to date:** Läuft der Server mindestens auf einer sauberen PHP 8.x Version, für die es noch aktive globale Sicherheitsupdates gibt?

3. Backups (Die absolute Lebensversicherung)

- Remote-Speicherung:** Liegt das Backup physisch getrennt vom Webseite-Server (z.B. in Amazon S3 Cloud Drives, Google Drive, nicht lokal im wp-content-Ordner)?
- Automatisiert & Täglich:** Werden Datenbank UND Files (Bilder, Plugins) vollkommen automatisiert (z.B. nachts um 4 Uhr) über Tools wie Updraft gesichert?
- Wiederherstellung getestet:** Hast du aus dem Backup jemals probiert, einen Testserver wieder hochzufahren? Ein nie getestetes Backup ist genauso schlecht wie kein Backup.

Tipp der Profis: Bei jeder E-Mail zu WordPress-Erweiterungen mit dem Titel "Urgent Security Patch", die an den Server-Admin geht, nicht lange fragen. Updaten! Die "Guten" finden die Lücken, publizieren den Patch und von exakt da an, suchen die bösen Bots genau diese Lücken im Netz.

EIN INTERNES TOOL DER ROCKET WEBSITE GMBH • WWW.HAUPTSTADT-HOMEPAGE.DE