WordPress Security: Praktische Strategien

Reality-Check: Was wird am häufigsten angegriffen?

- Plugins - größtes Sicherheitsrisiko
- Themes - veraltet, Nulled Themes (illegale Kopien)
- Login-Bereich - Brute Force
- WordPress Core - wenn veraltet
- Datenbank - SQL Injection

First Things First

- Regelmäßige Updates von WordPress, Plugins und Themes
- Nur vertrauenswürdige Plugins und Themes aus offiziellen Quellen
- Inaktive Plugins & Themes löschen
- Starke Passwörter + 2FA

Tipp

- Passwortmanager verwenden - 1Password, Bitwarden
- Auto-Updates für Minor Releases aktivieren

Fundament: Hosting & Baseline

- PHP aktuell (>= 8.1), HTTPS aktiv, SFTP/SSH statt FTP
- Kein Benutzername „admin“, starke Passwörter, Benutzerrollen nur mit notwendigen Rechten vergeben
- Server-Backups beim Hoster aktiv?
- Site Health prüfen

Hinweise

- Dateirechte: Keine 777-Rechte
- Backups beim Hoster ≠ externen Backups - besser noch ein separates Remote-Backup

Welche Hinweise liefert Site Health?

- WordPress, Plugins, Themes aktuell
- PHP-Version aktuell
- HTTPS aktiv
- Inaktive Plugins/Themes vorhanden
- Hintergrund-Updates/Loopback-Requests blockiert
- REST-API-Probleme, fehlende PHP-Module (z. B. imagick)
- Datenbank- und Server-Konfiguration – Hinweise bei nicht optimalen Einstellungen.

Edge (optional): Cloudflare Free als Schutzschicht

- DDoS-Schutz
- Managed Ruleset
- Bot Fight Mode
- 5 Firewall-Regeln
- Kostenloses SSL Zertifikat

Hinweise

- DSGVO beachten
- Für sehr kleine Seiten möglicherweise überdimensioniert

App-Schutz: Schlanke Firewall statt All-in-One

- SQL-Injection
- Cross-Site Scripting (XSS)
- Remote/Local File Inclusion (RFI/LFI)
- Command Injection / Shellcode
- File Upload Exploits
- Realtime-Blocking
- Logs & Reports
- **Keine Cloud-Abhängigkeit**

Hardening Teil 1: Login & Konten

- **2FA einrichten**
  Plugin “Two-Factor”
- **Login-Versuche limitieren**
  Plugin “Protect Login”
- **Passwort-Regeln durchsetzen**
  Plugin “Protect Login”
- **XML-RPC Schnittstelle deaktivieren**
  wenn nicht gebraucht

Hardening Teil 2: WordPress-Konfiguration wp-config.php

- define('DISALLOW_FILE_EDIT', true)
- define('FORCE_SSL_ADMIN', true)
- define('WP_AUTO_UPDATE_CORE', 'minor');
- SALTs erneuern (WordPress Salt Generator) - macht bestehende Sessions ungültig, alle müssen sich neu anmelden

Hinweise als Einsteiger besser lassen

- Tabellenpräfix ändern - (kaum Nutzen, Fehlerquelle)
- Manuelles Rechte-Tuning ohne Not

Was sind SALTs

- SALTs sind zufällige Zeichenketten, die WordPress nutzt, um sensible Daten kryptografisch zu schützen.
- Sie werden zusammen mit den sogenannten AUTH-Keys verwendet.
- Das Ziel: Selbst wenn jemand Zugriff auf deine Datenbank hat, kann er sich nicht einfach einloggen oder Cookies entschlüsseln.

Backups & Recovery

- Plugin wie z.B. UpdraftPlus oder WPvivid Free
- DB täglich
- Dateien wöchentlich
- Backup vor jedem größeren Update
- Remote Speicher (Google Drive, Dropbox…)
- Backup Restore regelmäßig testen - z.B. auf Subdomain
- Aufbewahrung mind. 30 Tage (wegen versteckter Malware)

Wie kann ich meine Backups auf Fehler überprüfen bzw. einen Restore-Test machen?

1. Testumgebung anlegen – z. B. lokale Installation oder Staging-Server
2. Restorefunktion des Backup-Plugins nutzen bzw. händisch einspielen (Schritte 3-5)
3. Backup herunterladen (Dateien + Datenbank)
4. Dateien entpacken und hochladen
5. Datenbank importieren (z. B. über phpMyAdmin)
6. Website im Browser öffnen und prüfen: Startseite, Login, Bilder, Menüs, Formulare

Monitoring & Routine

- Schwachstellen & Malware Check - Patchstack Free (Plugin), Sucuri SiteCheck, Ninja Scanner (Plugin), ManagedWP

Routine

- Wöchentlich - Updates checken
- Monatlich - Malware-Scan, Backup-Test
- Quartalsweise -Plugin-Inventur (Was brauche ich wirklich?)

Tipps

- Major Updates lieber manuell und besser mit Staging-Test
- Backup **VOR** jedem größeren Update

„Security in 60 Minuten“: Minimal-Plan

- **Hosting**
  PHP aktuell, HTTPS, Site Health ok
- **Login**
  2FA aktivieren, Protect Login
- **WAF**
  NinjaFirewall aktivieren
- **Hardening**
  DISALLOW_FILE_EDIT, FORCE_SSL_ADMIN, SALTs erneuern, XML-RPC aus (wenn nicht nötig)
- **Backups**
  UpdraftPlus/WPvivid, DB täglich, Files wöchentlich, Remote-Speicher
- **Auto-Updates**
  für Minor Releases aktivieren
- **Routine**
  Updates, monatlicher Mini-Restore-Test

Links & More

https://github.com/bigod/wordpress-security