Sicherheits-Checkliste für WordPress

1. Sichere Zugangsdaten verwenden

- Wähle ein starkes Passwort (mindestens 12 Zeichen, inkl. Zahlen, Groß- und Kleinbuchstaben sowie Sonderzeichen).
- Ändere den Standard-Benutzernamen „admin“ zu etwas Individuellem.
- Aktiviere die Zwei-Faktor-Authentifizierung (2FA).

2. WordPress, Themes und Plugins aktuell halten

- Aktualisiere regelmäßig WordPress, installierte Themes und Plugins.
- Entferne nicht verwendete Themes und Plugins, um Angriffspunkte zu reduzieren.

3. Sicherheits-Plugins installieren

- Nutze Plugins wie „Wordfence Security“ oder „Sucuri Security“, um Angriffe zu erkennen und abzuwehren.
- Konfiguriere die Firewall und aktiviere automatisierte Malware-Scans.

4. Backups erstellen

- Setze ein Backup-Plugin wie „UpdraftPlus“ oder „BackupBuddy“ ein.
- Speichere Backups regelmäßig auf externen Speichermedien oder in der Cloud.

5. Sichere Verbindung nutzen

- Installiere ein SSL-Zertifikat, um die Kommunikation zwischen Server und Besuchern zu verschlüsseln (https:// statt http://).
- Prüfe die SSL-Verschlüsselung mit Tools wie „SSL Labs“.

6. Login-Beschränkungen einrichten

- Begrenze die Anzahl der Login-Versuche, um Brute-Force-Angriffe zu verhindern.
- Nutze Plugins wie „Limit Login Attempts Reloaded“.

7. Verzeichnisschutz aktivieren

- Schütze sensible Dateien wie wp-config.php durch spezielle Server-Einstellungen.
- Deaktiviere die Anzeige des Verzeichnisinhalts (Directory Listing) in der .htaccess-Datei.

8. Regelmäßige Sicherheitsüberprüfung

- Überprüfe deine Seite regelmäßig auf Schadsoftware und Sicherheitslücken.
- Tools wie „SiteCheck“ von Sucuri können dir dabei helfen.

9. Sichere Hosting-Umgebung

- Wähle einen sicheren Hosting-Anbieter, der auf WordPress spezialisiert ist.
- Prüfe, ob das Hosting automatische Sicherheitsupdates und DDoS-Schutz bietet.

10. Nutzerrollen und Rechte verwalten

- Weisen den Benutzern nur die Rechte zu, die sie wirklich benötigen.
- Lösche ungenutzte Benutzerkonten.