

Website Security Checkliste

Basis-Sicherheit (Hohe Priorität)

- SSL/HTTPS aktivieren & erzwingen
- Starke Admin-Passwörter einrichten (min. 12 Zeichen, komplexe Zeichen)
- Automatische Updates aktivieren (CMS, Plugins, Themes)
- DSGVO-Basics implementieren (Datenschutzerklärung, Cookie-Banner)
- Backup-System einrichten (täglich DB, wöchentlich komplett)

Erweiterte Sicherheit (Mittlere Priorität)




- Web Application Firewall konfigurieren (DDoS & Injection Schutz)
- Zwei-Faktor-Authentifizierung für Admin-Accounts
- Security-Plugins installieren (Malware-Scanner, Brute-Force-Schutz)
- Sichere Dateiübertragung einrichten (SFTP)
- Content Security Policy (CSP) implementieren

Monitoring & Wartung

- Server-Monitoring einrichten (Performance, Uptime)
- Log-Dateien regelmäßig prüfen (Zugriffe, Fehler)
- Vierteljährliche Security-Scans durchführen
- Zugriffsrechte regelmäßig überprüfen
- Incident Response Plan bereithalten

Documentation & Wartung

- System- & Prozessdokumentation pflegen
- Zugangsdaten sicher verwalten (Passwort-Manager)
- Wiederherstellungsprozeduren dokumentieren
- Kontakte für Notfälle aktuell halten
- Mitarbeiter regelmäßig schulen

Prioritäten:  Hoch (sofort) |  Mittel (diese Woche) |  Niedrig (dieser Monat)