

SSL & Server Security

1. Basis Sicherheit (SSL)

- ☐ Ein gültiges SSL/TLS-Zertifikat ist installiert (Let's Encrypt / Premium).
- ☐ Gesamter Traffic wird serverseitig von HTTP via 301 Weiterleitung zwangsweise auf HTTPS umgeleitet.
- ☐ HSTS (HTTP Strict Transport Security) Header ist gesetzt, damit Browser nur verschlüsselte Verbindungen zulassen.

2. Applikationsschutz & CMS

- ☐ Die Standard-Login-Seiten (z.B. /wp-admin) sind durch Limit-Login-Attempts (Schutz vor Brute-Force) gesichert oder per .htaccess maskiert.
- ☐ Web Application Firewall (WAF) wie Cloudflare oder ein Plugin zur Abwehr bösartiger POST-Requests aktiv.
- ☐ Keine sensiblen Testordner oder "index.php.bak" Backup Dateien öffentlich abrufbar.

3. Backups & Disaster Recovery

- ☐ Tägliche, inkrementelle Backups auf einen externen (Cloud-)Speicherplatz und unabhängig vom gleichen Server (AWS S3, Dropbox, etc).
- ☐ Datenbank wird in noch kürzeren Intervallen im Loop gesichert.
- ☐ Ein getesteter "Notfall"-Plan zur schnellen Rückspielung eines Backups existiert.