

Website-Sicherheit: Checkliste für Betreiber

PRAXISLEITFADEN | Stand: 27. Oktober 2026 | Kostenlos

1. HTTPS und Transport

Vorgehen: Prüfe gültiges Zertifikat, HTTP→HTTPS-Weiterleitung und gemischte Inhalte. HSTS erst nach Prüfung aller betroffenen Subdomains ausrollen.

Beispiel: `curl -I http://example.org` und `curl -I https://example.org`

Prüfkriterium: HTTP leitet sauber um, keine Mixed-Content-Warnungen.

Vermeiden: HSTS includeSubDomains ohne Inventar aktivieren.

2. Updates und Abhängigkeiten

Vorgehen: Erfasse CMS, Plugins, PHP-Laufzeit und Libraries. Aktualisiere nach Test und Backup; entferne ungenutzte Komponenten.

Beispiel: `composer audit` für PHP-Abhängigkeiten.

Prüfkriterium: Bekannte kritische Sicherheitslücken sind bewertet und behandelt.

Vermeiden: Nur das CMS, aber nicht Plugins und Laufzeit aktualisieren.

3. Zugänge und MFA

Vorgehen: Beschränke Admin-Konten, verwende individuelle Konten und MFA, wo unterstützt. Prüfe Rollen und ausscheidende Mitarbeiter.

Beispiel: Admin-Rollenliste mit Eigentümer und letzter Prüfung.

Prüfkriterium: Kein gemeinsames Administratorpasswort im Umlauf.

Vermeiden: Dauerhaft geteilte Logins ohne Nachvollziehbarkeit.

4. Header und Sitzungen

Vorgehen: Prüfe CSP, X-Content-Type-Options, Referrer-Policy und Cookie-Attribute. Starte CSP bei komplexen Seiten gegebenenfalls mit Report-Only.

Beispiel: `Set-Cookie: session=...; Secure; HttpOnly; SameSite=Lax`

Prüfkriterium: Keine unnötigen Scriptquellen, Cookies passend abgesichert.

Vermeiden: Blind kopierte CSP, die Geschäftsprozesse blockiert.

5. Backups und Wiederherstellung

Vorgehen: Sichere Dateien und Datenbank getrennt und teste eine Wiederherstellung in einer isolierten Umgebung.

Beispiel: Monatlicher Restore-Test mit Protokoll und Zeitmessung.

Prüfkriterium: Ein dokumentierter Restore funktioniert mit aktuellen Sicherungen.

Vermeiden: Backup-Erfolgsmeldung ohne Restore-Test als Sicherheit ansehen.

Fachquellen

OWASP Cheat Sheet Series – <https://cheatsheetseries.owasp.org/>

Onlineversion: <https://www.cyberknecht.de/wissen/checklisten/website-sicherheit-checkliste.html>