Published on *internetaces* (https://internetaces.com)

Drupal Website-Sicherheit verbessern – Umfassende Strategien und Praxis-Tipps im Jahr 2025

Drupal Website Sicherheit 2025

Cyberangriffe nehmen stetig zu und stellen Unternehmen vor große Herausforderungen. Um Vertrauen, Funktionalität und Nutzerfreundlichkeit sicherzustellen, ist es unerlässlich, Ihre Website wirksam zu schützen. In diesem Leitfaden erfahren Sie, welche Maßnahmen Sie ergreifen sollten, um die Sicherheit Ihrer Website deutlich zu verbessern.

Warum ist die Absicherung Ihrer Website unverzichtbar?

Cyberkriminalität wächst rasant: Experten rechnen damit, dass die weltweiten Schäden durch Cyberattacken bis 2028 auf über 13 Billionen US-Dollar steigen könnten. Websites und Web-Apps zählen dabei zu den bevorzugten Zielen von Hackern, weshalb ein umfassender Schutz essentiell geworden ist.

- **Verlust vertraulicher Daten:** Sicherheitslücken können sensible Kundendaten preisgeben und

erheblichen finanziellen sowie rechtlichen Schaden verursachen.
- **Unterbrechung der Erreichbarkeit:** DDoS-Angriffe und Hackerattacken beeinträchtigen die Zugänglichkeit Ihrer Website und führen zu Umsatzverlusten sowie einem schlechten Nutzererlebnis.
- **Image-Schäden:** Cybervorfälle schädigen das Ansehen eines Unternehmens nachhaltig, wie prominente Fälle großer Datenlecks gezeigt haben.

Grundlegende Sicherheitsmaßnahmen für jede Website

SSL-Zertifikate und HTTPS-Verbindungen

SSL-/TLS-Zertifikate verschlüsseln die Datenübertragung zwischen Nutzern und Servern. Dadurch schützen sie vertrauliche Informationen wie Passwörter, Zahlungsdaten und persönliche Informationen vor unbefugtem Zugriff. Zudem belohnen Suchmaschinen HTTPS-geschützte Seiten mit besseren Rankings.

Regelmäßige Softwareaktualisierungen

Veraltete Software gehört zu den häufigsten Sicherheitsrisiken. Aktualisieren Sie Ihr CMS, Plugins und andere Systeme kontinuierlich, um bekannte Schwachstellen rechtzeitig zu schließen.

- Aktivieren Sie automatische Updates, wenn möglich.
- Löschen Sie ungenutzte Plugins und Themes.
- Bleiben Sie über Sicherheitswarnungen Ihres CMS informiert.

Mehrstufige Authentifizierung (MFA)

MFA erhöht die Sicherheit durch eine zweite Authentifizierungsebene, wie temporäre Codes aus Authenticator-Apps oder physische Sicherheitsschlüssel (z.B. YubiKey). Dadurch verhindern Sie effektiv unberechtigte Zugriffe, selbst wenn Passwörter gestohlen wurden.

Regelmäßige Datensicherungen

Automatisierte Backups ermöglichen die schnelle Wiederherstellung im Schadensfall. Wichtig ist dabei:

- Backups für Dateien und Datenbanken getrennt durchführen.
- Sicherungen an mehreren Orten, etwa Cloud-Diensten, ablegen.
- Backups regelmäßig testen, um ihre Funktionsfähigkeit sicherzustellen.

Web Application Firewalls (WAF) und DDoS-Schutz

Eine WAF filtert schädliche Zugriffe wie SQL-Injektionen oder XSS-Angriffe heraus. Kombinieren Sie diese mit speziellen DDoS-Abwehrdiensten (z.B. Cloudflare), um größere Angriffe effektiv abzuwehren.

Website-spezifische Sicherheitseinstellungen

Passwortsicherheit erhöhen

Nutzen Sie sichere Passwörter mit hoher Komplexität und verwenden Sie Passwortmanager, um die Verwaltung sicherer Passwörter zu erleichtern. Ergänzend bietet MFA zusätzlichen Schutz.

E-Mail-Benachrichtigungen bei Kontoänderungen

Aktivieren Sie automatische E-Mail-Alarme bei Änderungen von Passwörtern, E-Mail-Adressen und Zugriffsrechten, um frühzeitig auf potenzielle Bedrohungen reagieren zu können.

Sitzungsbegrenzung und automatischer Logout

Richten Sie automatische Logout-Funktionen ein, um Sitzungen nach einer definierten Zeit der Inaktivität zu schließen und damit Risiken durch verwaiste Sitzungen zu reduzieren.

Schutz des Login-Bereichs

Implementieren Sie CAPTCHA-Lösungen und begrenzen Sie Login-Versuche, um Brute-Force-Attacken effektiv abzuwehren.

Sicherheitsorientierte HTTP-Header

Spezielle HTTP-Sicherheitsheader wie X-Frame-Options, HSTS und Content Security Policy stärken den Schutz auf Browserebene und verhindern verschiedene Angriffstypen wie Clickjacking oder XSS.

Warum Drupal als besonders sicheres CMS gilt

Drupal überzeugt durch regelmäßige Sicherheitsupdates, strenge Coding-Standards und eine aktive Community. Granulare Rollen- und Zugriffsrechte erhöhen den Schutz deutlich und machen Drupal zu

einer idealen Wahl für sicherheitskritische Webprojekte.

Sicherheitsmodule in Drupal

- **Password Policy:** Erzwingt sichere Passwörter.
- **Captcha/reCAPTCHA:** Verhindert automatisierte Angriffe.
- **Security Kit:** Aktiviert HTTP-Header zur Verteidigung gegen XSS und Clickjacking.
- **Automated Logout:** Meldet Nutzer automatisch ab.
- **Login Security:** Begrenzung von Login-Versuchen und verbesserte Authentifizierung.

Schnelle Sicherheitsimplementierung in Drupal

Mithilfe vorgefertigter Sicherheitspakete (wie DDR Security Recipe) lässt sich eine umfassende Absicherung schnell und unkompliziert vornehmen.

Fazit und nächste Schritte

Ein solides Sicherheitskonzept kombiniert technische Maßnahmen mit kontinuierlicher Überwachung und regelmäßigen Audits. Durch die Umsetzung der hier genannten Strategien können Sie Risiken deutlich reduzieren und die Integrität sowie Vertrauenswürdigkeit Ihrer Website dauerhaft gewährleisten. Für komplexe Anforderungen empfiehlt sich zudem die Zusammenarbeit mit erfahrenen Sicherheitsexperten.

Kategorie:
Allgemein [1]
Drupal [2]
Tags:
Sicherheit [3]
Drupal-Security [4]

Links
[1] https://internetaces.com/de/blog-kategorien/allgemein
[2] https://internetaces.com/de/blog-kategorien/drupal
[3] https://internetaces.com/de/tags/sicherheit
[4] https://internetaces.com/de/tags/drupal-security