

## Online Business mit WordPress – Schritt 15 = WordPress absichern

Kategorien : [WordPress](#)

Schlagwörter : [WordPress](#)

Datum : 6. Dezember 2016



In diesem r23Artikel möchten wir einige wichtige und interessante Tipps geben, wie man sein Online Business mit WordPres sicher aufbaut. Mit Tipps zur Sicherheits-Maximierung, die auch bei unseren Kundenprojekten Anwendung finden.

**Dieser Artikel ist Teil einer Artikelserie:**

[Artikelserie zum Thema Online Business mit WordPress](#)

[Schritt 1 = Planung und Vorbereitung](#)

[Schritt 2 = Domainname](#)

[Schritt 3 = Content Planung](#)

[Schritt 4 = WordPress Installation](#)

[Schritt 5 = Piwik Installation](#)

[Schritt 6 = Verschiedene Nutzerkonten einrichten](#)

[Schritt 7 = WordPress Einstellungen](#)

[Schritt 8 = Suchmaschinenoptimierung für mehr Kunden & Umsatz](#)

[Schritt 9 = Beiträge optimieren mit dem SEO Plugin von Yoast](#)

[Schritt 10 = WordPress Plugins für Einsteiger](#)

[Schritt 11 = Keyword-Planer](#)

[Schritt 12 = Soziale Netzwerke in Yoast SEO konfigurieren](#)

[Schritt 13 = Personal Branding - Die ICH-Marke](#)

[Schritt 14 = WordPress Themes - Responsive Webdesign](#)

**Schritt 15 = WordPress absichern**

Schritt 16 = Blog-Vermarktung

## WordPress Sicherheit

Sicherheit wird bei WordPress sehr ernst genommen, aber wie bei jedem anderen System können potentielle Sicherheitsrisiken zu einem Problem werden, wenn grundlegende Sicherheitsregeln missachtet wurden. Dieser r23Artikel behandelt typische Schwachstellen und was man tun kann, um die eigene WordPress-Installation abzusichern.

Sollten dir die WordPress Absicherung dennoch nicht gelingen, dann kannst du dich gerne bei uns über das [Support Forum](#) melden. Es ist eine kostenlose Anmeldung erforderlich, um Fragen zu posten.

## Inhaltsverzeichnis

1. [BSI veröffentlicht Sicherheitsstudie](#)
2. [Der richtige Host](#)
3. [WordPress: Sicherheit von Anfang an](#)
4. [Tipps zum Umgang mit Passworten](#)
5. [WordPress, Themes und Plugins aktuell halten](#)
6. [.htaccess nutzen zur Erhöhung der Sicherheit](#)
7. [Blog gehackt, was tun? | Eine Schnellhilfe für das gehackte WordPress Blog](#)
8. [Weblinks / Empfehlungen](#)

## BSI veröffentlicht Sicherheitsstudie

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat eine Studie zur Sicherheit von Content Management Systemen veröffentlicht. Diese beleuchtet relevante Bedrohungslagen und Schwachstellen der weit verbreiteten Open-Source-CMS Drupal, Joomla!, Plone, TYPO3 und **WordPress**.

Die Studie bietet unter anderem eine Analyse der Schwachstellen der untersuchten CMS. Zudem werden die Entwicklungsprozesse der Systeme mit dem Fokus auf Sicherheit untersucht und bewertet. Darüber hinaus ermöglicht die Studie eine verlässliche sicherheitstechnische Beurteilung von CMS im Rahmen der Planung und Beschaffung.

Der PDF Download Link der BSI Sicherheitsstudie findet ihr auf folgender Seite.

[BSI Sicherheitsstudie zu Content Management Systemen](#)

## Der richtige Hoster

Der richtige Hoster kümmert sich um alle Sicherheits- und Core-Updates vom WebServer. Er hält PHP auf den aktuellen Stand und pflegt den Server. Außerdem erstellt er jede Nacht ein voll automatisches Backup deiner Webseiten und speichert dieses ohne Mehrkosten für dich! Zusätzlich kannst du ein manuelles Backup anlegen.

**Backups sind Pflicht!** Sollte dein Hoster kein Backup anbieten, dann ist es Zeit den Hoster zu wechseln.

## WordPress: Sicherheit von Anfang an

Die Absicherung von WordPress fängt bereits bei der [Installation](#) an. Nur sichere [Passwörter](#) bieten ausreichenden Schutz.

[WordPress Installation](#)

## Tipps zum Umgang mit Passwörtern

- Lasse dein Passwort niemand anderen benutzen, auch nicht System-Administratoren.
- Schreibe dein Passwort nicht auf.
- Klebe dein Passwort nicht auf den Monitor oder unter die Tastatur.
- Speichere dein Passwort nicht auf dem Computer.
- Verschicke dein Passwort nicht über E-Mail.
- Wechsel dein Passwort regelmäßig.
- Speichere dein Passwort nicht in Cloud-Diensten externer Anbieter.

Der Online-Passwort-Generator [passwort-generator.de](https://passwort-generator.de) erzeugt online beim Aufruf sechs unterschiedlich lange Passwörter (30, 26, 22, 18, 14, 10 Zeichen Länge) von untadeliger Qualität.

## WordPress, Themes und Plugins aktuell halten

Alle Sicherheitsmaßnahmen nützen nichts, wenn man ein uraltes System mit veralteten Plugins oder Themes betreibt. WordPress, Themes und Plugins solltet ihr zeitnah aktualisieren und so stets auf aktuellem Stand halten. Wer sich nicht oft in das Dashboard einloggt und gerne eine Benachrichtigung über neue Updates erhält, kann sich das Plugin [WP Updates Notifier](#) installieren.

## .htaccess nutzen zur Erhöhung der Sicherheit

Sind Skripte nicht dafür vorgesehen, vom Anwender abgerufen zu werden, kann man eine weitere Sicherheitsstufe einbauen. Ein Weg ist, diese Skripte mit mod\_rewrite in der .htaccess-Datei zu blockieren. Hinweis: Damit der nachfolgende Code nicht von WordPress überschrieben wird, sollte er in der .htaccess außerhalb des Abschnitts platziert werden, der mit # BEGIN WordPress anfängt und # END WordPress endet. WordPress kann alles innerhalb dieser Tags überschreiben.

```
# Block the include-only files.      RewriteEngine On RewriteBase / RewriteRule ^wp-admin/includes/ - [F,L] RewriteRule !^wp-includes/ - [S=3] RewriteRule ^wp-includes/[^/]+\.(php|css|js)$ - [F,L] RewriteRule ^wp-includes/js/tinymce/langs/.+\.(php|css|js) - [F,L] RewriteRule ^wp-includes/theme-compat/ - [F,L] # BEGIN WordPress
```

Wenn du unsere [Installations-Anleitung](#) aus dieser Artikelserie bei der Installation verwendest hast, so haben wir diese notwendige Änderungen für dich bereits durchgeführt.

Des Weiteren verhindert unser .htaccess das Ausführen von PHP Skripten in dem upload Verzeichnis und noch einiges mehr.

.htaccess aus unserem Projekt auf GitHub

## WordPress auf Schwachstellen und Konfigurationsfehler prüfen

Für deine WordPress-Installation habe ich ein Leistungspaket im Angebot:

- Prüfung deiner WordPress-Installation auf Schwachstellen
- Auswertung und Beurteilung der gefundenen Schwachstellen
- Absicherung deiner WordPress-Installation

Wenn du Deine WordPress-Installation nachhaltig absichern möchtest, kannst Du [mich gerne kontaktieren](#).

## Blog gehackt, was tun? | Eine Schnellhilfe für das gehackte WordPress Blog

Wenn deine Website gehackt oder mit Malware infiziert wurde, solltest du schnell reagieren, um den Schaden zu beheben. Du schadest nicht nur dich selbst, sondern vielleicht auch anderen mit einer gehackten Website!

Google stellt einen Leitfaden zur Verfügung: [Hilfe, ich wurde gehackt! | Google Developers](#)

## Weblinks / Empfehlungen

[de:WordPress absichern « WordPress Codex](#)

BSI Sicherheitsstudie zu Content Management Systemen

[Blog gehackt, was tun? | Eine Schnellhilfe für das gehackte WordPress Blog](#)

[Passwörter](#)

[Online-Passwort-Generator](#)

## Jetzt bist du gefragt!

Welche empfehlenswerte Security-Maßnahmen, die nicht in meinem Artikel enthalten sind, nutzt ihr?

Du kannst diesen Beitrag natürlich auch weiterempfehlen. Ich bin dir für jede Unterstützung dankbar!

(Bild: [Macrovector](#) / [Shutterstock.com](#))

## **Verwandeln Sie Ihren Commerce mit AR und 3D-Produktvisualisierung!**

Bei uns geht es um Techniken, die es schaffen, das Produkt zum Erlebnis zu machen. Virtual & Augmented Reality, 360 Grad-Videos, Darstellungen in 3D, virtuelle Showrooms. Die Besucher:innen sollen eintauchen in die Welt des Unternehmens mit immersiven Technologien.



Sie können uns mit der Erstellung von individuellen 3D-Visualisierungen beauftragen. Jeder kann 3D-Visualisierungen bei unserem Kreativservice bestellen - unabhängig davon, ob Sie nur ein einzelnes 3D-Modell benötigen oder viele.

Wir unterstützen Sie bei der Umsetzung Ihres Augmented Reality (AR) oder Virtual Reality (VR) Projektes! Egal ob [Produktfotografie](#), [3D Scan Service](#), [3D-Visualisierung](#) oder fertige [3D Modelle für AR/VR](#) – wir beraten Sie persönlich und unverbindlich.

### **Wo kann ich Anregungen, Lob oder Kritik äußern?**

Ihre Meinung ist uns wichtig! Schreiben Sie uns, was Ihnen in Bezug auf unser Angebot bewegt. [info@r23.de](mailto:info@r23.de)

## R23 — Ihr Atelier für Virtual Reality und interaktive Markenerlebnisse

Wünschen Sie ein individuelles Angebot auf Basis Ihrer aktuellen Vorlagen, nutzen Sie einfach unser [Anfrageformular](#).

## Online Business mit WordPress – Schritt 15 = WordPress absichern



<https://blog.r23.de/online-business-mit-wordpress-schritt-15-wordpress-absichern/>

Besuchen Sie uns auch auf [Facebook](#) und [Twitter](#).

r23  
Thüringenstr. 20  
58135 Hagen  
Deutschland  
Telefon: 02331 / 9 23 21 29

E-Mail: [info@r23.de](mailto:info@r23.de)

Ust-IdNr.:DE250502477