Wie Sie verkaufen, auch wenn Sie teurer sind

Wie Sie verkaufen, auch wenn Sie teurer sind – websiteboosting.com

Zugegeben, aktuell geht es der Digitalwirtschaft sehr gut. Zum einen wissen viele Kunden um die Wichtigkeit ihres digitalen Auftritts Bescheid, zum anderen unterstützt der Staat zusätzlich mit zahlreichen Förderprogrammen Investitionen – und damit auch so manche Agentur. Doch egal, wie die…
Zugegeben, aktuell geht es der Digitalwirtschaft sehr gut. Zum einen wissen viele Kunden um die Wichtigkeit ihres digitalen Auftritts Bescheid, zum anderen unterstützt der Staat zusätzlich mit zahlreichen Förderprogrammen Investitionen – und damit auch so manche Agentur. Doch egal, wie die aktuellen Konstellationen sind: Es wird immer Agenturen geben, die teurer als andere sind. Vielleicht gehören auch Sie zu den Höherpreisigen. Dann ist die entscheidende Frage: Wie erfolgreich schließen Sie Aufträge ab, wenn Sie nicht der billigste Anbieter sind? Oder knicken Sie gar am Ende der Verhandlung ein und geben zahlreiche Leistungen gratis, weil Sie nicht in der Lage sind, Ihren Preis auf Augenhöhe zu erklären?

So manche Gründer orientieren sich bei der Preisfindung an ihren Mitbewerbern: Was nehmen diese pro Stunde? Wie sehen deren Angebote aus? Im Ergebnis ist dann deren Angebot für Außenstehende oft austauschbar. Denn wenn Webseiten, Imagebroschüren und auch die Mitarbeiter alle die gleichen Phrasen dreschen – woran soll sich dann ein Kunde orientieren? Erst recht dann, wenn ein potenzieller Abnehmer wenig Ahnung von der Materie hat und zwangsläufig einen objektiven Vergleich zwischen beispielsweise drei Agenturen nicht machen kann, wird sich dieser oft für den günstigsten entscheiden müssen. Denn wie soll ein Kunde seinen eigenen Kollegen erklären, dass er nicht das billigste Angebot gekauft hat, sondern das teurere für 10.000 Euro mehr, wenn er das Angebot und das Konzept dahinter nicht wirklich versteht? Sie können davon ausgehen, dass manche Kunden bei Ihrem günstigeren

Mitbewerber kaufen, obwohl Sie eigentlich den Auftrag wirklich verdient hätten, weil Sie ihm nicht ausreichend verdeutlichen konnten, dass Sie Ihren Preis wirklich(!) wert sind.

Am Anfang steht die Bedarfsanalyse

Das Wichtigste im Verkaufsgespräch, die Bedarfsanalyse, wird selbst von Profi-Verkäufern oft unterschätzt. Eine schlechte Bedarfsanalyse rächt sich spätestens bei der Preisverhandlung. Denn wie wollen Sie argumentieren, wenn Sie nicht wissen, was Ihrem Kunden wichtig ist? Bei einer guten Bedarfsanalyse laufen Sie bildlich gesprochen im Kopf des Anfragenden herum, um diesen vollumfänglich zu verstehen. Sie wissen nach dieser Analyse, was Ihr Kunde will und nicht will. Sie wissen danach, woran Ihr Kunde festmacht, dass Sie seinen Auftrag gut erledigt haben – und dass er Ihren Preis respektiert und akzeptiert. Aufgrund der Antworten können Sie dann auch für sich entscheiden, ob Sie diesen Kunden überhaupt haben wollen – oder nicht. Oder etwas spitzer formuliert: Sie müssen nach der Bedarfsanalyse ganz klar für sich entscheiden, ob Sie es verantworten können, den Auftrag zu übernehmen. Denn wenn zwei Personen einen Vertrag unterschreiben, dann müssen beide Seiten auch liefern.
Teilen Sie die Bedarfsanalyse auf wenigstens(!) zwei Termine auf. Den ersten Termin führen Sie online oder telefonisch durch. Finden Sie bei diesem Gespräch Antworten auf mindestens folgende fünf Fragen:

- Was haben Sie genau vor?
- Weshalb?
- Ab wann soll das Ganze fertig sein?
- Welche Erfahrungen haben Sie bisher mit Agenturen gemacht?
- Wie sind Ihre finanziellen Vorstellungen?

Hauptziel dieses Erstgespräches ist es, dass Sie danach ganz

klar sagen können: „Ja, es macht Sinn, weitere Zeit in das Projekt zu investieren“, oder: „Dafür sind wir nicht die Richtigen. Hier können wir es nicht verantworten, den Auftrag zu übernehmen.“ Im letzteren Fall sollten Sie den Kunden nicht im Regen stehen lassen, sondern im Idealfall an eine andere Agentur weiterempfehlen.

Kunden wollen Sicherheit

Aber nicht nur Sie müssen den Anfragenden „abklopfen“, sondern Sie müssen sich auch richtig inszenieren. Und zwar so, dass im zeitlichen Verlauf der Verkaufsabschluss zu Ihren kalkulierten Preisen das Ergebnis ist. Es bringt wenig, wenn Sie mit Interessenten langweilige Logosammlungen Ihrer zufriedenen Kunden durchgehen. Denn nur weil Sie Logos von Kunden veröffentlichen, bedeutet das ja noch lange nicht, dass Sie diese Kunden auch wirklich begeistert haben. Darüber hinaus sagt ein Logo auch recht wenig über die Größe des Projekts aus. Fragen Sie sich besser, welche Sorgen und Ängste potenzielle Kunden haben:

- Haben die mich wirklich verstanden?
- Können die das wirklich?
- Wie verhalten die sich, wenn Probleme auftreten?
- Gibt es unangenehme Überraschungen (finanzieller oder zeitlicher Art)?
- Was passiert, wenn ich während der Zusammenarbeit merke, dass ich mich für den falschen Anbieter entschieden habe?
- Sollte ich jetzt kaufen – oder bekomme ich diese Leistung auch irgendwo anders billiger oder besser?
- Wie viel „Luft“ ist noch in den Preisen?
- Was sagen die anderen Agenturen, die ich auch angefragt habe, wenn ich mich jetzt gegen diese entscheide?
- Wie werden meine Kollegen reagieren, wenn ich die falsche Agentur beauftrage?

- Wäre es besser, gar keine Agentur zu beauftragen – und alles so zu lassen, wie es jetzt ist?

Auf diese Fragen, die sich nahezu jeder potenzielle Kunde mehr oder weniger bewusst stellt, geben die meisten Anbieter von sich aus kaum gute Antworten. Zwangsläufig verlaufen so manche Anfragen im Sand. Denn wer hat noch nicht beim Nachfassen Sätze gehört wie: „Wir lassen erst mal alles so, wie es ist“, oder: „Wir haben jetzt andere Themen auf der Agenda. Melden Sie sich gerne in einem halben Jahr wieder, dann haben wir dafür wieder den Kopf frei“?

> *Der Preis ist egal, wenn die Gegenleistung stimmt.*

Vorbereitung Preisverhandlung

Egal, ob Sie mit neuen Kunden verhandeln oder mit bestehenden: Bereiten Sie sich auf Preisgespräche immer vor. Stellen Sie sich folgende Fragen:

1. Wie verdient der Kunde eigentlich sein Geld? Was sind auf Sicht der nächsten Monate und Jahre Probleme und Aufgaben, auf die er zusteuert?
2. Wie hoch ist eigentlich sein tatsächliches Einkaufsvolumen? Arbeitet er beispielsweise noch mit einer weiteren Agentur zusammen?
3. Was ist der Grund, dass der Kunde den Preis verhandeln möchte – und nicht etwas anderes?
4. Was sind unsere Ziele bei der Preisverhandlung?
5. Wie lange soll der verhandelte Preis gültig bleiben?
6. Wer nimmt alles an der Preisverhandlung teil?
7. Was lief bisher gut bei der Zusammenarbeit? Was nicht?
8. Mit welchen Möglichkeiten kann die Beziehung zu den Verhandlungspartnern verbessert werden?
9. Was sind mögliche Argumente aus Kundensicht, um einen niedrigeren Preis zu bekommen?

10. Welche Sonderleistungen wurden in der Vergangenheit nicht berechnet?
11. Mit welchen Argumenten verteidigen bzw. erklären Sie Ihren Preis?
12. Welche sinnvollen Alternativen zu einem Preisnachlass können dem Kunden angeboten werden?
13. Was sind mögliche Nachteile für den Kunden, wenn er nicht mit uns zusammenarbeitet?
14. Wie kann dem Kunden geholfen werden, Geld zu sparen oder mehr Geld zu verdienen?
15. Was ist der Plan B, wenn es bei der Verhandlungsrunde zu keinem Ergebnis kommt?

Verkäufer dürfen keine Schönredner sein

Sie sind für das verantwortlich, was Sie verkaufen, aber auch für das, was Sie nicht verkaufen. Das muss Ihnen ganz klar sein. Sie dürfen sich niemals aus der Verantwortung mit Sätzen wie: „Hätte der Kunde ja sagen können, dass er das so meint“, oder: „Hat er mir ja nicht gesagt, dass ihm x wichtig ist“, aus der Verantwortung stehlen. Denn im Zweifelsfalle bekommen Sie immer die Schuld, auch wenn Sie diese objektiv vielleicht gar nicht haben. Oder glauben Sie, dass ein Kunde, der sich von Ihnen schlecht beraten fühlt, in seinem Umfeld sagt: „Ja, und dann habe ich mich für die Agentur x entschieden. Denen habe ich leider vergessen zu sagen, dass mir a und b sehr wichtig sind. Das hat den gesamten Zeitplan zerfetzt und zu Mehrkosten von 30.000 Euro geführt“? Nein, Ihr Kunde wird in seinem Umfeld sagen: „Geh bloß nicht zu der Agentur x. Die können das nicht. Labern rum, kommen aber nicht in die Pötte. Letztlich musste ich denen noch 30.000 Euro nachschießen, weil die keine Ahnung haben.“ Klingt hart, aber so ist die Realität.
Darum müssen Sie nicht nur im Rahmen der Auftragsklärung

vieles zur Verständnisförderung hinterfragen, sondern gegebenenfalls auch klare Grenzen ziehen. Beispielsweise mit Sätzen wie: „Nein, so machen wir das nicht, weil …“, oder: „Wir könnten das in so einer einfachen Version machen, wie Sie das wünschen. Das wollen wir aber nicht, weil Sie dann nicht Ihre Ziele erreichen. Und letztlich können wir es uns nicht erlauben, Sie besseren Wissens ins offene Messer laufen zu lassen. Wir machen das also entweder richtig oder sonst lieber gar nicht. Denn wir haben auch eine Verantwortung dafür, dass Sie Ihr Geld gut investieren.“ Für manche Anbieter sind das „scharfe Aussagen“, die sie sich leider nicht zu sagen trauen. Doch wenn Sie dies wertschätzend und wohlwollend und nicht arrogant rüberbringen, dann wird so manch ein Kunde denken: „Die wissen, was sie wollen. Die scheinen ihr Geschäft zu verstehen. Also sind das wohl die richtigen Partner für mich, die ihr Geld wert sind.“

Verkaufen ist Erwartungsmanagement

Viele Kunden sind sich gar nicht darüber im Klaren, wie viel Arbeit und auch Kosten auf sie zusätzlich zukommen. Als schlechter Verkäufer werden Sie das auch von sich aus nicht kommunizieren. Als souveräner Verkäufer durchaus. Es geht nicht darum, den Kunden zu belehren, sondern ihn vielmehr zu informieren. Denn je offener die Karten sind, mit denen Sie spielen, umso harmonischer verläuft auch die Geschäftsbeziehung. Das bedeutet, dass Sie nicht nur einen klaren Zeitplan mit Ihrem Kunden gemeinsam(!) erstellen, bis wann er was geliefert haben muss, sondern dass Sie auch offensiv und rechtzeitig kommunizieren, wenn etwas von Ihrer Seite aus nicht eingehalten werden kann.

Feilschen macht Spaß

Was sagen Sie eigentlich spontan, wenn Ihr (potenzieller) Kunde zu Ihnen sagt: „Am Preis müssen wir noch was machen?“

Und Ihre Kollegen? Viele Verkäufer sind nicht in der Lage, auf diese elementare Frage souverän(!) zu antworten. So machen dann viele Anbieter ihr eigenes Unvermögen zum Problem des Kunden. Denn wenn dieser eine Antwort hört, die ihm nicht das Gefühl gibt, dass der Preis so in Ordnung ist, dann wittert er schnell die Chance auf Preisnachlässe. Es ist elementar, dass Sie nicht nur gute Antworten haben, sondern diese auch glaubwürdig (Stichworte sind hier Stimme, Modulation, Blickkontakt, …) kommunizieren.
Es gibt viele Gründe, warum Kunden um Preisnachlässe feilschen:

- Test, ob noch „Luft“ in den Preisen ist.
- Sicherheit, nicht zu viel zu bezahlen.
- Mitbewerber bietet günstiger an.
- Einfach andere Vorstellungen vom Wert des Angebots.
- Begrenztes Budget.
- Gebot der Wirtschaftlichkeit, den besten Preis zu bekommen.
- Einkäufer haben die Aufgabe, Preise zu drücken.
- Oft kommen Nachlässe nur, weil man danach fragt.
- Spaß und Lust am Feilschen.
- Macht ausleben.

Insbesondere die letzten beiden Faktoren spielen die Hauptrolle bei Preisverhandlungen. Darum sollten Sie sich vor voreiligen Zugeständnissen hüten. Denn andernfalls denkt so manch ein Kunde: „Das war ja einfach. Ich habe einmal gefragt und bekomme jetzt schon einen Preisnachlass. Wie viel geht der denn nun noch runter, wenn ich ihn noch zwei Wochen zappeln lasse?“

> *Wenn der Kunde nicht feilscht, dann hast du zu billig angeboten.*

Antworten auf „zu teuer!“

Ein Angebot muss nicht zwangsläufig zu teuer sein, nur weil der Kunde dies sagt. Möglicherweise sind die vorgestellte Lösung und der erwartete Nutzen für den Kunden zu gering und deswegen im Verhältnis zur Leistung zu teuer. Hier ein paar Formulierungsbeispiele zur Inspiration.

1. Natürlich kann ich Ihnen beim Preis entgegenkommen. Soll ich Ihnen A oder lieber B aus dem Angebot rausrechnen?
2. Wie kommen Sie darauf?
3. Wenn Sie jetzt ein wenig mehr investieren, rechnet es sich mittelfristig besser für Sie. Schauen Sie hier …
4. Ja, billig sind wir nicht. Billig wäre es, wenn …
5. Ja, zuerst scheint der Preis ein wenig hoch zu sein. Lassen Sie uns bitte noch einmal zusammenfassen, welches Leistungspaket für Sie dahintersteckt.

Antworten auf „Mitbewerber ist billiger!“

Einkäufer müssen sich eventuell auch intern rechtfertigen, weshalb sie nicht bei dem billigsten, sondern bei einem anderen gekauft haben. Darum braucht der Einkäufer häufig nur gute Argumente vom Verkäufer, um sich intern ggf. erklären zu können. Formulieren Sie doch mal folgende Ideen in Ihren Worten um und probieren Sie aus:

1. Unser Mitbewerber ist sein Geld durchaus wert. Mehr allerdings auch nicht. Darf ich Ihnen kurz aufzeigen, was uns entscheidend von diesem abhebt?
2. Jetzt mal Hand aufs Herz. Wir würden uns doch nicht so lange unterhalten, wenn es Ihnen nur um den Preis ginge, oder?
3. Oh, das ist interessant. Haben Sie schon herausgefunden,

woran die sparen, um solche Preise machen zu können? Denn auch die können ja nicht vom Verschenken leben, oder?

Über den Preis kann jeder reden

Auch wenn es respektlos klingt, aber „zu teuer!“ kann jeder sagen. Auch jemand, der vom Thema gar keine Ahnung hat. Im schlimmsten Falle versteht also Ihr Gegenüber gar nicht, was Sie mit seinem Geld für ihn alles Gutes tun wollen. Er sieht nur Ihr Angebot, Ihren Preis – und denkt: „Das Einzige, was ich hier verstehe, ist, dass die viel Geld haben wollen. Also rede ich nur über den Preis.“
Dazu wenden manche Kunden auch interessante Tricks an. Das ist legitim. Denn auch Verkäufer nutzen ja mehr oder weniger bewusst psychologische Tricks, um den Abschluss zu machen.

- Appell über die Beziehung: Wenn man sich kennt, dann kann man doch auch nett zueinander sein. Also warum nicht einen Preisnachlass geben?
- Guter Cop, böser Cop: Einer auf der Kundenseite spielt den wohlwollenden Kunden, der andere den kritischen. Vorher haben sich beide aufgrund Ihres schriftlich eingereichten Angebots über 20.000 Euro auf 18.500 Euro verständigt. Nun fordert der böse Cop von Ihnen, vielleicht auch mit etwas Drama und spitzer Argumentation, einen Preis von 15.000 Euro. Der gute Cop vermittelt zwischen Ihnen wohlwollend und schlägt 18.500 Euro vor. Erfreut über diesen Kompromissvorschlag stimmen Sie diesem Preis zu. Ein Preiszugeständnis, welches Sie ohne den bösen Cop vermutlich niemals gegeben hätten.
- Salamitaktik: Hier fordert der Kunde immer weitere Zugeständnisse. Stimmen Sie ihm beispielsweise zu, dass die Einweisung seiner Mitarbeiter nicht berechnet wird, wird er gleich den nächsten Punkt nachverhandeln,

beispielsweise die monatliche Wartungspauschale. Denken Sie, nachdem Sie hier auch entgegengekommen sind, dass es nun endlich den Auftrag gibt, wird der nächste Punkt aufs Korn genommen.

Viele Anbieter erkaufen sich Aufträge über Rabatte bzw. Leistungen, die dann „ausnahmsweise“ nicht berechnet werden. Das rächt sich in der unternehmerischen Bilanz schnell. Denn das, was nicht eingenommen wird, kann auch nicht zum Gewinn beitragen oder für unternehmerisch wichtige Investitionen beispielsweise in die Mitarbeiterentwicklung genutzt werden.

Verkaufen Sie souverän

Alle Mitarbeiter mit Kundenkontakt müssen(!) kommunikativ geschult sein. Andernfalls besteht das Risiko, dass diese nicht nur eine Zumutung für die Kunden werden, sondern auch eine Gefahr für Ihre gesamte Unternehmung. Denn Menschen mit Kundenkontakt beeinflussen entscheidend Ihre unternehmerischen Bilanzen. Von diesen ist es abhängig, ob der Kunde den Preis leicht akzeptiert, ob er aggressiv reklamiert oder Sie mit Überzeugung weiterempfiehlt. Dass Sie Ihren Job beherrschen, setzt ein Kunde voraus. Er möchte aber die Sicherheit haben, dass Sie ein Geschäftspartner auf Augenhöhe sind und Ihren Preis wert sind.
Wer sich seiner eigenen Stärken bewusst ist, diese auch so erklären kann, dass (potenzielle) Kunden sie leicht verstehen, darüber hinaus auch wertschätzende Antworten parat hat, wenn es mal einen kritischen Einwand gibt, wird eine gute Beziehung aufbauen – und den Auftrag machen.

Disable and Remove Google Fonts

Disable and Remove Google Fonts

Von Fonts Plugin

Beschreibung

Verbessert die Leistung der Website, indem Google Fonts deaktiviert werden, die von Themes oder Plugins geladen werden.

While this plugin removes Google Fonts from as many themes and plugins as possible, some require additional steps, we have detailed those here: Remove Google Fonts from WordPress

Plugin-Kompatibilität

Dieses Plugin funktioniert mit allen WordPress-Themes. Speziell getestet wurde es für folgende Themes:

- Twenty Twelve
- Twenty Thirteen
- Twenty Fourteen
- Twenty Fifteen
- Twenty Sixteen
- Twenty Seventeen
- Twenty Nineteen
- Twenty Twenty
- Avada
- Enfold

- Sydney
- Hestia
- Hueman
- Vantage
- ColorMag
- Shapely
- OnePress
- JupiterX
- Storefront
- Divi Extra
- Zerif Lite

Es entfernt auch Google Fonts, die von den folgenden Plugins geladen werden:

- Divi
- MailPoet
- Elementor
- Beaver Builder
- Revolution Slider
- WPBakery (Visual Composer)

Neben der Verbesserung der Ladezeit kann das Entfernen der Google Fonts auch dazu beitragen, die Bestimmungen der DSGVO einzuhalten.

Fehler

Wenn du ein Problem mit diesem Plugin feststellst, melde dich bitte hier!

Mitwirkende

Jeder ist willkommen, zu diesem Plugin beizutragen.

Es gibt verschiedene Arten, wie du dich beteiligen kannst:

1. Melde uns Fehler, die du feststellst.

2. Übersetze „Disable and Remove Google Fonts“ in verschiedene Sprachen
3. Gib uns Feedback und mache Vorschläge für Verbesserungen

FAQ

Wird mein Theme mit „Disable and Remove Google Fonts“ funktionieren?

Site Kit by Google – Analytics, Search Console, AdSense, Speed

Site Kit by Google – Analytics, Search Console, AdSense, Speed

Von Google

Version: **1.87.0** Zuletzt aktualisiert: **vor 3 Tagen** Aktive Installationen: **2+ Millionen** WordPress-Version: **4.7 oder höher** Getestet bis: **6.1** PHP-Version: **5.6 oder höher** Sprachen: Schlagwörter:

adsenseanalyticsgooglepagespeed insightsSearch Console

Beschreibung

Site Kit is the official WordPress plugin from Google for insights about how people find and use your site. Site Kit is the one-stop solution to deploy, manage, and get insights from critical Google tools to make the site successful on the web. It provides authoritative, up-to-date insights from multiple Google products directly on the WordPress dashboard for easy access, all for free.

Bringt die besten Google-Dienste zu WordPress

Site Kit includes powerful features that make using these Google products seamless and flexible:

- Easy-to-understand stats directly on your WordPress dashboard
- Offizielle Statistiken verschiedener Google-Werkzeuge, alle in einem Dashboard
- Quick setup for multiple Google tools without having to edit the source code of your site
- Metrics for your entire site and for individual posts
- Easy-to-manage, granular permissions across WordPress and different Google products

Unterstützte Google-Tools

Site Kit shows key metrics and insights from different Google products:

- **Search Console:** Understand how Google Search discovers and displays your pages in Google Search. Track how many people saw your site in Search results, and what query they used to search for your site.
- **Analytics:** Explore how users navigate your site and track goals you've set up for your users to complete.
- **AdSense:** Keep track of how much your site is earning

you.

- **PageSpeed Insights:** See how your pages perform compared to other real-world sites. Improve performance with actionable tips from PageSpeed Insights.
- **Tag Manager:** Use Site Kit to easily set up Tag Manager- no code editing required. Then, manage your tags in Tag Manager.
- **Optimize:** Use Site Kit to easily set up Optimize- no code editing required. Then, set up A/B tests in Optimize.

FAQ

Für weitere Informationen, besuche die offizielle Site Kit Website.

Ist Site Kit kostenlos?

What are the minimum requirements for Site Kit?

Why is my dashboard showing “gathering data” and none of my service data?

Why aren’t any ads appearing on my site after I connected AdSense?

Is Site Kit GDPR compliant?

Where can I get additional support?

Mitwirkende & Entwickler

„Site Kit by Google – Analytics, Search Console, AdSense, Speed“ ist Open-Source-Software. Folgende Menschen haben an diesem Plugin mitgewirkt:

WordPress – SICHERHEIT – So bereinigen Sie eine gehackte WordPress

How to Clean a Hacked WordPress Site using Wordfence – Wordfence

If your site has been hacked, Don't Panic. This article will describe how to clean your site if it has been hacked and infected with malicious code, backdoors, spam, malware, or other nastiness. This article was updated in December of 2021 with additional resources to help clean specific infection t… Wenn Ihre Website gehackt wurde, geraten Sie nicht in Panik.

In diesem Artikel wird beschrieben, wie Sie Ihre Website bereinigen, wenn sie gehackt und mit bösartigem Code, Hintertüren, Spam, Malware oder anderen schädlichen Inhalten infiziert wurde. Dieser Artikel wurde im Dezember 2021 mit zusätzlichen Ressourcen zur Beseitigung bestimmter Infektionstypen aktualisiert. Dieser Artikel wurde von Mark Maunder, dem Gründer von Wordfence, geschrieben. Ich bin ein akkreditierter Sicherheitsforscher, ein CISSP, ein WordPress-Entwickler und der Geschäftsführer von Defiant Inc, dem Hersteller von Wordfence. Auch wenn Sie kein WordPress verwenden, enthält dieser Artikel mehrere Tools, mit denen Sie Ihre Website von einer Infektion befreien können.

Wenn Sie WordPress verwenden und gehackt wurden, können Sie Wordfence verwenden, um einen Großteil des Schadcodes von Ihrer Website zu entfernen. Mit Wordfence können Sie Ihre gehackten Dateien mit den ursprünglichen WordPress-Kerndateien und den Originalkopien von WordPress-Themes und -Plugins im Repository vergleichen. Mit Wordfence können Sie sehen, was sich geändert hat, und haben die Möglichkeit, Dateien mit einem Klick zu reparieren oder zu löschen.

Wenn Sie ein vielbeschäftigter Geschäftsinhaber sind und möchten, dass sich unser erfahrenes Team um das Problem kümmert, melden Sie sich jetzt bei Wordfence Care auf den Link „Hilfe anfordern", an und klicken Sie dann auf der Lizenzseite um sofort eine Anfrage zur Website-Bereinigung zu stellen .

Wenn Sie eine geschäftskritische Website haben und diese sofort oder außerhalb der regulären Geschäftszeiten gereinigt werden muss, melden Sie sich jetzt bei Wordfence Response an und stellen Sie eine Website-Reinigungsanfrage. Unser 24-Stunden-Team zur Reaktion auf Vorfälle wird innerhalb einer Stunde mit der Arbeit beginnen. Sie reagieren unglaublich schnell und lösen das gesamte Problem innerhalb von 24 Stunden. Gehen Sie wie bei Wordfence Care nach der Anmeldung zur Seite „Lizenzen“ und klicken Sie bei Ihrer Lizenz auf „Hilfe anfordern“. Sie gelangen dann in die Prioritätswarteschlange für Response-Kunden.

Wenn Sie sich selbst um das Problem kümmern möchten oder Wordfence Care oder Response nicht in Ihrem Budget liegt, lesen Sie weiter. WIR KÖNNEN DAS SCHAFFEN!! Das Bereinigen Ihrer gehackten Website ist einer der Gründe, warum ich Wordfence erstellt habe. Die kostenlose Version von Wordfence enthält leistungsstarke Tools, die Ihnen beim Bereinigen Ihrer Website helfen.

Wurden Sie wirklich gehackt?

Wenn Sie vermuten, dass Sie gehackt wurden, stellen Sie zunächst sicher, dass Sie tatsächlich gehackt wurden. Manchmal wenden sich Website-Administratoren in Panik an uns und denken, sie seien gehackt worden, obwohl sich ihre Website einfach nur schlecht verhält, ein Update fehlgeschlagen ist oder ein anderes Problem auftritt. Manchmal sehen Websitebesitzer Spam-Kommentare und können den Unterschied zwischen diesen und einem Hack nicht erkennen.

Ihre Website wurde gehackt, wenn:

- In der Kopf- oder Fußzeile Ihrer Website wird Spam angezeigt, der Werbung für Dinge wie Pornografie, Drogen, illegale Dienste usw. enthält. Oftmals wird dieser Spam in den Inhalt Ihrer Seite eingefügt, ohne

dass an die Darstellung gedacht wurde, sodass er möglicherweise als dunkler Text auf einer Seite erscheint Der Hintergrund muss dunkel sein und für das menschliche Auge nicht gut sichtbar sein (die Suchmaschinen können ihn jedoch erkennen).

- Sie führen eine Site:example.com-Suche (ersetzen Sie example.com durch Ihre Website) bei Google durch und sehen Seiten oder Inhalte, die Sie nicht kennen und die bösartig aussehen.
- Sie erhalten Berichte von Ihren Benutzern, dass sie auf eine bösartige oder Spam-Website weitergeleitet werden. Achten Sie besonders darauf, da viele Hacks erkennen, dass Sie der Site-Administrator sind, und Ihnen keine Spam-Inhalte anzeigen, sondern Spam nur Ihren Besuchern oder den Suchmaschinen-Crawlern anzeigen. Versuchen Sie, beim Besuch Ihrer Website ein Inkognito-Fenster zu verwenden oder Ihre Website über ein Suchergebnis zu besuchen, anstatt die URL direkt einzugeben.
- Sie erhalten von Ihrem Hosting-Anbieter eine Meldung, dass Ihre Website böswillige oder Spam-Aktivitäten ausführt. Wenn Ihr Host Ihnen beispielsweise mitteilt, dass er Berichte über Spam-E-Mails erhält, die einen Link zu Ihrer Website enthalten, kann dies bedeuten, dass Sie gehackt wurden. Was die Angreifer in diesem Fall tun, besteht darin, Spam von irgendwoher zu versenden und Ihre Website als Link zu verwenden, um Personen auf eine Website umzuleiten, die ihnen gehört. Sie tun dies, weil das Einfügen eines Links zu Ihrer Website Spamfilter umgeht, während das Einfügen eines Links zu ihrer eigenen Website von Spamfiltern erfasst wird.

Wordfence erkennt viele dieser Probleme sowie andere, die ich hier nicht erwähnt habe. Achten Sie daher auf unsere Warnungen und reagieren Sie entsprechend.

Sichern Sie jetzt Ihre Website. Hier ist der Grund:

Sobald Sie festgestellt haben, dass Sie gehackt wurden, sichern Sie sofort Ihre Website. Verwenden Sie FTP, das Backup-System Ihres Hosting-Anbieters oder ein Backup-Plugin, um eine Kopie Ihrer gesamten Website herunterzuladen. Sie müssen dies tun, da viele Hosting-Anbieter Ihre gesamte Website sofort löschen, wenn Sie melden, dass sie gehackt wurde, oder wenn sie schädliche Inhalte entdecken. Klingt verrückt, oder? In manchen Fällen ist dies jedoch ein Standardverfahren, um zu verhindern, dass andere Systeme in ihrem Netzwerk infiziert werden.

Stellen Sie sicher, dass Sie auch Ihre Website-Datenbank sichern. Die Sicherung Ihrer Dateien und Datenbank sollte Ihre erste Priorität sein. Wenn Sie dies erledigen, können Sie sicher mit dem nächsten Schritt der Bereinigung Ihrer Website fortfahren und dabei beruhigt sein, dass Sie zumindest eine Kopie Ihrer gehackten Website haben und nicht alles verlieren.

Dinge, die Sie wissen sollten, bevor Sie eine gehackte WordPress-Site bereinigen:

Hier sind die Verkehrsregeln für die Reinigung Ihrer Website:

- Normalerweise können Sie alles im wp-content/plugins/-Verzeichnis löschen, ohne dass dabei Daten verloren gehen oder Ihre Website beschädigt wird. Dabei handelt es sich um Plugin-Dateien, die Sie neu installieren können, sodass Sie keine Daten löschen, die Sie nicht einfach ersetzen können. Wenn Sie diese Dateien löschen, erkennt WordPress automatisch, dass Sie ein Plugin gelöscht haben und deaktiviert es. Es wird also nicht

zum Absturz Ihrer Website führen. **Stellen Sie einfach sicher, dass Sie in wp-content/plugins ganze Verzeichnisse löschen und nicht nur einzelne Dateien.** Wenn Sie beispielsweise das Wordfence-Plugin löschen möchten, müssen Sie wp-content/plugins/wordfence und alles in diesem Verzeichnis löschen, einschließlich des Verzeichnisses selbst. Wenn Sie nur ein paar Dateien aus einem Plugin löschen, kann Ihre Website möglicherweise nicht mehr funktionsfähig sein.

- Normalerweise haben Sie nur ein Theme-Verzeichnis, das für Ihre Site im Verzeichnis wp-content/themes verwendet wird. Wenn Sie wissen, welches das ist, können Sie alle anderen Theme-Verzeichnisse löschen. **Beachten Sie, dass Sie bei einem „untergeordneten Thema" möglicherweise zwei Verzeichnisse in wp-content/themes verwenden** . Dies ist keine übliche Konfiguration.
- Den Verzeichnissen wp-admin und wp-includes werden sehr selten neue Dateien hinzugefügt. Wenn Sie also in diesen Verzeichnissen etwas Neues finden, ist die Wahrscheinlichkeit hoch, dass es bösartig ist.

Achten Sie auf alte WordPress-Installationen und Backups. Wir sehen oft infizierte Websites, bei denen jemand sagt: „Aber ich habe meine Website auf dem neuesten Stand gehalten und ein Sicherheits-Plugin installiert, warum wurde ich also gehackt?" Manchmal passiert es, dass Sie oder ein Entwickler eine Kopie aller Ihrer Site-Dateien in einem Unterverzeichnis wie /old/ sichern, auf das über das Internet zugegriffen werden kann. Dieses Backup wird nicht gepflegt und obwohl Ihre Hauptseite sicher ist, kann ein Angreifer auf die alte Seite zugreifen, sie infizieren und über die von ihm installierte Hintertür auf Ihre Hauptseite zugreifen. Lassen Sie also **niemals alte WordPress-Installationen herumliegen. Wenn Sie gehackt werden, überprüfen Sie diese zuerst, da sie wahrscheinlich voller Malware sind.**

Ein paar nützliche Tools:

Wenn Sie SSH-Zugriff auf Ihren Server haben, melden Sie sich an und führen Sie den folgenden Befehl aus, um alle Dateien anzuzeigen, die in den letzten 2 Tagen geändert wurden. Beachten Sie, dass der Punkt das aktuelle Verzeichnis angibt. Dadurch durchsucht der folgende Befehl das aktuelle Verzeichnis und alle Unterverzeichnisse nach kürzlich geänderten Dateien. Um herauszufinden, was Ihr aktuelles Verzeichnis ist, wenn Sie SSH verwenden, geben Sie „pwd“ ohne Anführungszeichen ein und drücken Sie die Eingabetaste.

```
find . -mtime -2 -ls
```

Oder Sie können ein bestimmtes Verzeichnis angeben:

```
find /home/yourdirectory/yoursite/ -mtime -2 -ls
```

Oder Sie können die Suche ändern, um Dateien anzuzeigen, die in den letzten 10 Tagen geändert wurden:

```
find /home/yourdirectory/yoursite/ -mtime -10 -ls
```

Wir empfehlen Ihnen, die obige Suche durchzuführen und die Anzahl der Tage schrittweise zu erhöhen, bis Sie geänderte Dateien sehen. Wenn Sie selbst nichts geändert haben, seit Sie gehackt wurden, ist es sehr wahrscheinlich, dass Sie die Dateien sehen, die der Angreifer geändert hat. Sie können sie dann selbst bearbeiten oder löschen, um den Hack zu bereinigen. Dies ist bei weitem die effektivste und einfachste Methode, um herauszufinden, welche Dateien infiziert wurden, und wird von jedem professionellen Website-Reinigungsdienst verwendet.

Ein weiteres nützliches Tool in SSH ist „grep“. Um beispielsweise nach Dateien zu suchen, die auf die Base64-Kodierung verweisen (häufig von Hackern verwendet), können Sie den folgenden Befehl ausführen:

```
grep -ril base64 *
```

Dadurch werden nur die Dateinamen aufgelistet. Sie können die Option „l“ weglassen, um den tatsächlichen Inhalt der Datei anzuzeigen, in der die Base64-Zeichenfolge vorkommt:

```
grep -ri base64 *
```

Bedenken Sie, dass „base64“ auch in legitimem Code vorkommen kann. Bevor Sie etwas löschen, sollten Sie sicherstellen, dass Sie keine Datei löschen, die von einem Theme oder Plugin auf Ihrer Website verwendet wird. Eine verfeinerte Suche könnte so aussehen:

```
grep --include=*.php -rn . -e "base64_decode"
```

Dieser Befehl durchsucht alle Verzeichnisse und Unterverzeichnisse nach Dateien, die auf .php enden, durchsucht sie nach der Textzeichenfolge „base64_decode“ und gibt alle gefundenen Ergebnisse einschließlich der Zeilennummer aus, sodass Sie leicht finden können, wo sie in jeder Datei vorkommt .

Nachdem Sie nun wissen, wie man „grep“ verwendet, empfehlen wir Ihnen, grep in Kombination mit „find“ zu verwenden. Was Sie tun sollten, ist, Dateien zu finden, die kürzlich geändert wurden, zu sehen, was in der Datei geändert wurde, und wenn Sie eine häufige Textzeichenfolge wie „bad hacker was here“ finden, können Sie einfach alle Ihre Dateien wie folgt nach diesem Text durchsuchen:

```
grep -irl "bad hacker was here" *
```

und das zeigt Ihnen alle infizierten Dateien, die den Text „bad hacker was here“ enthalten. Vergessen Sie nicht das Sternchen (den Stern) am Ende des letzten Befehls.

Ich habe dir gesagt, dass wir das schaffen können! Ich bin mir sicher, dass Sie sich zu diesem Zeitpunkt wegen Ihrer gehackten Website viel weniger gestresst fühlen, da Sie jetzt

über ein paar Tools zum Sortieren schädlicher Dateien aus Ihrer regulären WordPress-Installation verfügen.

Gehen wir noch tiefer! Wenn Sie viele infizierte Websites bereinigen, werden Sie Muster bemerken, an denen sich häufig bösartiger Code befindet. Ein solcher Ort ist das Upload-Verzeichnis in WordPress-Installationen. Der folgende Befehl zeigt Ihnen, wie Sie alle Dateien im Upload-Verzeichnis finden, die keine Bilddateien sind. Die Ausgabe wird in einer Protokolldatei namens „uploads-non-binary.log“ in Ihrem aktuellen Verzeichnis gespeichert.

```
find public_html/wp-content/uploads/ -type f -not -name "*.jpg" -not -name "*.png" -not -name "*.gif" -not -name "*.jpeg" -not -name “*.webp” >uploads-non-binary.log
```

Beachten Sie den Verzeichnispfad direkt nach dem Befehl „find“ oben. Wir gehen davon aus, dass Ihr aktuelles Verzeichnis Ihr Home-Verzeichnis auf Ihrem Webserver ist. Wir gehen außerdem davon aus, dass sich Ihre Website in public_html/ direkt neben diesem Home-Verzeichnispfad befindet. Denken Sie daran, dass Sie „pwd“ eingeben können, um herauszufinden, in welchem Verzeichnis Sie sich gerade befinden. Sie können auch „ls“ eingeben, um alle Dateien in Ihrem aktuellen Verzeichnis anzuzeigen, oder „ls -la“, um die Dateien in Ihrem aktuellen Verzeichnis mit weiteren Daten anzuzeigen jede Datei, wie Berechtigungen, Besitzer und wann die Datei zuletzt geändert wurde.

Mit den beiden einfachen Befehlszeilentools „grep“ und „find“ können Sie häufig eine ganze infizierte Website bereinigen. Wie einfach ist das! Ich wette, Sie sind jetzt bereit, Ihr eigenes Unternehmen für die Gebäudereinigung zu gründen.

So bereinigen Sie Ihre gehackte

WordPress-Site mit Wordfence:

Nachdem Sie nun einige leistungsstarke Tools in Ihrem Arsenal haben und bereits einige Grundreinigungen durchgeführt haben, starten wir Wordfence und führen einen vollständigen Scan durch, um Ihre Website zu bereinigen. Dieser Schritt ist wichtig, da Wordfence eine sehr komplexe Suche nach Infektionen durchführt. Zum Beispiel:

- Wir wissen, wie alle WordPress-Kerndateien, Open-Source-Themes und Open-Source-Plugins aussehen sollten, sodass Wordfence erkennen kann, ob eine Ihrer Quelldateien infiziert ist, selbst wenn es sich um eine neue Infektion handelt, die noch niemand zuvor gesehen hat. **Dies erreichen wir, indem wir die öffentlich verfügbaren Originaldateien mit Ihren Daten vergleichen und alle Änderungen kennzeichnen.** Es ist tatsächlich eine der coolsten Funktionen in Wordfence und völlig kostenlos!
- Wir suchen mithilfe komplexer regulärer Ausdrücke, die wir „Malware-Signaturen“ nennen, nach Anzeichen einer Kompromittierung. Unsere Malware-Signaturen werden basierend auf unserer Datenbank bekannter Infektionen kontinuierlich aktualisiert und unsere Premium-Kunden erhalten sofort die neuesten Signaturen. Mit einfachen Unix-Befehlszeilentools oder cPanel ist dies nicht möglich. Wir haben die besten Malware-Signaturen der Branche!
- Wir durchsuchen Ihre Dateien nach bekannten bösartigen Domänennamen, die häufig in Malware- und Spam-Dateien vorkommen.
- Wir verwenden SpamHaus, um festzustellen, ob die Domain oder IP-Adresse Ihrer Website zum Versenden von Spam verwendet wurde.
- Der Wordfence-Scan ist außerdem so konzipiert, dass er SEHR schnell läuft, wenn man bedenkt, wie viel Arbeit er macht, und sucht im Gegensatz zu generischen Scannern

gezielt nach WordPress-Malware.

So bereinigen Sie Ihre gehackte Website mit Wordfence:

1. Aktualisieren Sie Ihre Website auf die neueste Version von WordPress. Dies ist wichtig, da ältere Versionen von WordPress ungepatchte Schwachstellen aufweisen können.
2. Aktualisieren Sie alle Ihre Themes und Plugins auf die neuesten Versionen. Das Gleiche gilt auch hier. Entwickler beheben ständig Schwachstellen und Sicherheitsprobleme in Themes und Plugins. Besorgen Sie sich daher die neueste Version jedes Themes oder Plugins, das Sie verwenden.
3. Ändern Sie alle Passwörter auf der Website, insbesondere Administratorpasswörter. Wenn ein Benutzer oder, schlimmer noch, ein Administrator ein Passwort wiederverwendet hat, ist der Angreifer möglicherweise auf diese Weise überhaupt auf Ihre Website gelangt. Daher ist es wichtig, diese Änderung vorzunehmen.
4. Erstellen Sie ein weiteres Backup und speichern Sie es getrennt von dem oben empfohlenen Backup. Jetzt haben Sie eine infizierte Site, aber auf dieser Site wird die neueste Version von allem ausgeführt. Wenn beim Bereinigen Ihrer Website mit Wordfence etwas kaputt geht, können Sie zu dieser Sicherung zurückkehren und müssen nicht alle oben genannten Schritte erneut ausführen.
5. Stellen Sie sicher, dass Wordfence installiert ist. Die kostenlose Version reicht völlig aus, aber die Premium-Version bietet Ihnen die neuesten Malware-Signaturen und bösartigen Domänen.
6. Gehen Sie zum Wordfence-Menü „Scannen“ und klicken Sie einfach auf „Scan starten“. Dadurch wird ein erster Scan durchgeführt und Sie erhalten möglicherweise viele Ergebnisse, die Sie durcharbeiten müssen. Jedes Ergebnis erklärt, was Wordfence gefunden hat, und hilft Ihnen bei

der Lösung des Problems.

7. Sobald der Scan abgeschlossen ist und Sie die von Wordfence gefundenen Probleme behoben haben, können Sie einen noch tieferen Scan durchführen. Gehen Sie links zum Menü „Alle Optionen“. Scrollen Sie etwa zwei Drittel nach unten zur Überschrift „Grundlegende Scantypoptionen“ und aktivieren Sie das Kontrollkästchen, um „Hohe Empfindlichkeit“ zu aktivieren. Dadurch wird ein viel tiefergehender Scan durchgeführt, der etwas länger dauert, aber dieser Scan findet wirklich hartnäckige Malware, die schwerer zu erkennen und zu entfernen ist.
8. Wenn Sie zusätzliche Scans durchführen möchten, können Sie Ihren Wordfence-Scan auf der Seite „Alle Optionen“ genau an Ihre Bedürfnisse anpassen. Führen Sie so viele Scans durch, wie Sie möchten. Es gibt keine Begrenzung für die Anzahl der Scans, auch für unsere kostenlosen Kunden.
9. Wenn die Ergebnisse angezeigt werden, wird möglicherweise eine sehr lange Liste infizierter Dateien angezeigt. Nehmen Sie sich Zeit und arbeiten Sie die Liste langsam durch.
10. Untersuchen Sie alle verdächtigen Dateien und bearbeiten Sie diese entweder manuell, um sie zu bereinigen, oder löschen Sie die Datei. Denken Sie daran, dass Sie Löschungen nicht rückgängig machen können. Aber solange Sie das oben empfohlene Backup erstellt haben, können Sie die Datei jederzeit wiederherstellen, wenn Sie das Falsche löschen.
11. Sehen Sie sich alle geänderten Kern-, Theme- und Plugin-Dateien an. Verwenden Sie die von Wordfence bereitgestellte Option, um zu sehen, was sich zwischen der Originaldatei und Ihrer Datei geändert hat. Wenn die Änderungen bösartig aussehen, verwenden Sie die Wordfence-Option, um die Datei zu reparieren.
12. Arbeiten Sie sich langsam durch die Liste, bis sie leer ist.

13. Führen Sie einen weiteren Scan durch und bestätigen Sie, dass Ihre Website sauber ist.

anmelden, Wenn Sie weiterhin Hilfe benötigen, können Sie sich bei Wordfence Care um während der regulären Geschäftszeiten Hilfe zu erhalten, oder bei Wordfence Response , wenn Sie einen 24-Stunden-Service mit einer Reaktionszeit von 1 Stunde wünschen.

Ich habe eine Datei, die verdächtig aussieht, bin mir aber nicht sicher, ob sie es ist. Wie kann ich sagen?

Schicken Sie es uns per E-Mail an Samples@wordfence.com und wir informieren Sie. Wenn Ihre WordPress-Konfigurationsdatei wp-config.php infiziert ist, senden Sie keine Kopie dieser Datei an uns, ohne zuvor Ihre Datenbankanmeldeinformationen und die eindeutigen Authentifizierungsschlüssel und -salze zu entfernen.

Wenn Sie keine Antwort erhalten, hat entweder Ihr oder unseres E-Mail-System die Nachricht aufgrund Ihres Anhangs möglicherweise verworfen und geglaubt, sie sei bösartig. Senden Sie uns also bitte eine E-Mail ohne Anhang und teilen Sie uns damit mit, dass Sie uns etwas zusenden möchten. Wir werden dann mit Ihnen zusammenarbeiten, um die Probe zu erhalten.

Wo finde ich Hilfe bei der Beseitigung einer bestimmten Art

von Infektion?

Das Wordfence Learning Center bietet eine Reihe hilfreicher Artikel. Hier ist eine Liste von Artikeln, die Ihnen bei bestimmten Infektionsarten helfen:

- Entfernen bösartiger Weiterleitungen von Ihrer Website
- Hintertüren finden und entfernen
- Entfernen von Spam-Seiten von WordPress-Sites
- Spam-Links finden und entfernen
- Entfernen von Phishing-Seiten von WordPress-Sites
- Entfernen bösartiger Mailer-Codes von Ihrer Website
- Schädliche Datei-Uploader finden und entfernen
- Entfernung von WordPress-Defacement-Seiten
- So entfernen Sie verdächtigen Code von WordPress-Sites

Ich habe meine gehackte WordPress-Site bereinigt, aber Google Chrome zeigt mir immer noch die Malware-Warnung an. Was soll ich machen?

Sie müssen Ihre Website aus der Google Safe Browsing-Liste entfernen lassen. Dazu müssen Sie eine Bewertung bei Google anfordern. finden Sie auf dieser Seite in der Google-Dokumentation . Detaillierte Schritte dazu.

Besucher meiner Website erhalten Warnungen von

anderen Sicherheitsprodukten und Antivirensystemen. Was soll ich machen?

Der Verzicht auf die Google Safe Browsing-Liste ist ein großer Schritt, aber möglicherweise liegt noch einiges an Arbeit vor Ihnen. Sie müssen eine Liste aller Antivirenprodukte führen, die melden, dass Ihre Website infiziert ist. Dazu können Produkte wie ESET Antivirus, McAfee's Web Advisor und andere gehören.

Besuchen Sie die Website jedes Antiviren-Herstellers und finden Sie dort Anweisungen zum Entfernen Ihrer Website aus der Liste gefährlicher Websites. Dies wird von Antiviren-Herstellern oft als „Whitelisting" bezeichnet. Wenn Sie also nach Begriffen wie „Whitelisting", „Website-Entfernung", „False Positive" und dem Produktnamen googeln, gelangen Sie normalerweise zu der Stelle, an der Sie Ihre Website entfernen lassen können.

Wie kann ich manuell überprüfen, ob meine Website in der Safe Browsing-Liste von Google aufgeführt ist?

Besuchen Sie die folgende URL und ersetzen Sie example.com durch Ihre eigene Site-Adresse.

https://transparencyreport.google.com/safe-browsing/search?url=https://example.com/

Sie können ein Unterverzeichnis hinzufügen, wenn Ihre Site

über eines verfügt. Die angezeigte Seite ist sehr einfach, enthält jedoch detaillierte Informationen zum aktuellen Status Ihrer Website, warum sie in der Liste der sicheren Browser von Google aufgeführt ist und was als Nächstes zu tun ist.

Was tun, wenn Ihre Website sauber ist:

Glückwunsch!! Öffnen Sie auf jeden Fall Ihr Lieblingsgetränk und nehmen Sie einen großen Schluck! Jetzt müssen Sie sicherstellen, dass Ihre Website nicht erneut gehackt wird. Hier ist wie:

- Installieren Sie Wordfence und führen Sie regelmäßige Scans auf Ihrer WordPress-Site durch.
- Stellen Sie sicher, dass WordPress und alle Plugins und Themes auf dem neuesten Stand sind. Dies ist das Wichtigste, was Sie tun können, um Ihre Website zu sichern.
- Stellen Sie sicher, dass Sie sichere Passwörter verwenden, die schwer zu erraten sind.
- Aktivieren Sie die Zwei-Faktor-Authentifizierung. Wordfence bietet dies, sogar in unserer kostenlosen Version!
- Befreien Sie sich von allen alten WordPress-Installationen, die auf Ihrem Server herumliegen.
- Melden Sie sich für unsere WordPress-Sicherheitsmailingliste an , um über wichtige Sicherheitsupdates im Zusammenhang mit WordPress benachrichtigt zu werden. Dies ist eine E-Mail-Liste mit geringem Datenverkehr und hohem Signal-Rausch-Verhältnis, die sich auf die WordPress-Sicherheit konzentriert.
- Verbinden Sie Ihre Site mit Wordfence Central, um die Verwaltung der Sicherheit Ihrer Site erheblich zu

vereinfachen. Mit Central können Sie mit einem Klick einen Scan auf allen Ihren WordPress-Sites auslösen und die Sicherheitskonfiguration auf allen Ihren WordPress-Sites einfach verwalten. Ein effektives Konfigurationsmanagement ist eine äußerst effektive Möglichkeit, eine gehackte Website zu verhindern.

Vielen Dank, dass Sie dies gelesen haben, und ich hoffe, es hat Ihnen geholfen. auf Twitter markieren Wenn nicht, können Sie @wordfence oder mich direkt mit @mmaunder markieren .

Bleiben Sie gesund und munter!!

Mark Maunder – Gründer von Wordfence und CEO von Defiant Inc.

WordPress – SICHERHEIT – Experten Tipps

WordPress absichern wie ein Profi – Der komplette Guide

Wie Du WordPress absichern kannst wie ein

Profi | Experten Tipps

WordPress absichern 2022 ✔ Professionelle Tipps zur echten WordPress Sicherheit vom Experten ✔ Schritt für Schritt
Aktualisiert: 17.05.2023

Es kursieren sehr viele gut gemeinte Tipps im Netz, wie man WordPress absichern kann. Viele von ihnen taugen leider nicht viel. Denn echte WordPress Sicherheit gibt es nicht mit der einfachen Installation eines Plugins. Es ist ein Konzept von Maßnahmen, die aufeinander aufbauen. In diesem Beitrag zeige ich Dir, wie Du Dein WordPress bombensicher machst.

Inhaltsverzeichnis Anzeigen

Wenn Dir wirklich etwas an der WordPress Sicherheit liegt, dann solltest Du alle existierenden Sicherheitslücken schließen. Das kannst Du jedoch nur, wenn Dir bewusst ist, über welche Wege Dein WordPress angegriffen werden kann.

Erst dann leuchten die Maßnahmen ein und erst dann wird Dir bewusst, dass es keine Sicherheit mittels Plugin-Installation geben kann. Als **langjährige Experten** in der WordPress Sicherheit geben wir Dir heute Hintergrundwissen und eine Anleitung zur Absicherung Deines WordPress. Übrigens: Bis heute wurde keine Website gehackt, die wir abgesichert haben.

Dieses Tutorial ist nur für fortgeschrittene Anwender gedacht

und **nicht für Anfänger**. Du musst Dich auskennen mit FTP und der functions.php.

Auch interessant:

Cloud Sicherheit – Wie Du Dropbox und Co absichern kannst

WordPress Sicherheitslücken

Klären wir doch mal die wichtige Frage, über welche Wege WordPress überwiegend gehackt wird (und gehackt werden kann).

1. **Sehr leicht zu merkende und viel zu kurze Passwörter** (!)
2. **Veraltete WordPress-Versionen** – Mit jeder neuen Version werden die Sicherheitslücken der alten bekannt
3. **Veraltete Plugin-Versionen** – Auch Plugins haben eklatante Sicherheitslücken.
4. **Brute-Force Angriffe** gegen den Admin-Zugang
5. **Brute-Force Angriffe** gegen die xmlrpc.php Datei
6. **SQL-Injektionen** über Formulare
7. **Von außen zugängliche** WordPress-Dateien
8. Sicherheitslücke **WordPress REST-API (Update 26.05.2022)**

Zu 1: – WordPress Sicherheit fängt mit Deinem Passwort an

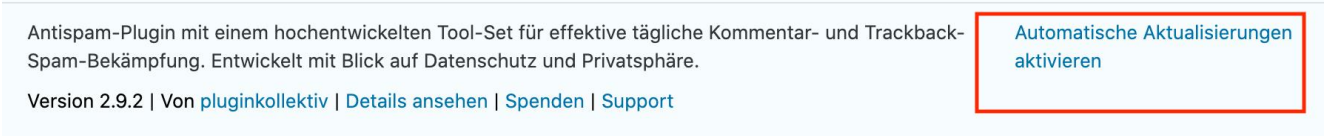
WordPress absichern ohne ein richtig gutes und wirklich sicheres Passwort hat leider überhaupt keinen Zweck. Alles, was leicht zu merken ist, ist auch leicht zu knacken. Und das wäre fatal. Deshalb sorge für ein anständiges Passwort aus Buchstaben, Zahlen, Sonderzeichen und Groß- und Kleinschreibung.

Ein gutes Passwort sollte schon 30stellig sein. Merken kann man sich das nicht mehr, aber es gibt ja Passwortmanager oder die entsprechenden Funktionen im Webbrowser.

Passwort-Generator aufrufen (externer Link)

Zu 2 + 3: – Die Updates

Das Du **WordPress und die Plugins aktuell halten** solltest und die Updates so schnell wie möglich ausführen solltest, hast Du bestimmt schon gelesen. Aber lesen bringt nichts. **Du musst es tun!** Ansonsten bettelst Du darum, gehackt zu werden. Zudem werden gern Plugins eingesetzt, die als beständig unsicher gelten – zum Beispiel der Revolution Slider. Übrigens kannst Du ab WordPress 5.5 Deine Plugins automatisch aktualisieren lassen.



Zu 4 + 5: – Brute-Force Angriffe

Hier versucht man mit der Brechstange Deine Zugangsdaten zu bekommen. Es werden zum Teil Tausende Variationen von Benutzernamen und Passwort ausprobiert. Diese Angriffe haben immer wieder Erfolg, weil der Benutzername meistens Admin ist und das Passwort kurz und gut zu merken ist.

Gern wird auch ein Angriff gegen die xmlrpc.php Datei ausgeführt, die zum Beispiel dazu dient, Beiträge per E-Mail veröffentlichen zu können. Auch über diese Datei kann man einen Vollzugriff auf die Website bekommen.

Was ist ein Brute-Force Angriff? (externer Link)

Zu 6: – SQL-Injektionen über Formulare

In ungeschützte Formulare (und auch direkt in der Adresszeile des Browsers) wird gern versucht Schadcode einzubringen. Hat das Erfolg, werden die Besucher Deiner Seite bereits durch einen einfachen Aufruf der Website mit Viren und Trojanern verseucht. Du wirst es erst merken, wenn Dein Webhoster die

Website abschaltet oder Google die Seite aus dem Index nimmt.

Was ist eine SQL-Injektion? (externer Link)

Zu 7: – Von außen zugängliche WordPress-Dateien

Nicht jeder Webhoster hat eine sichere Konfiguration seiner Hosting-Pakete oder Server. Manchmal sind WordPress-Dateien von außen zugänglich. Beliebte Angriffsziele sind hier zum Beispiel die install.php und die wp-config.php

Zu 8: – Die WordPress REST-API

Die REST-API bietet viele Möglichkeiten Inhalte auszulesen und diese können dann an externe Apps oder Websites übergeben werden. Dazu stellt die API strukturierte Daten (JSON) öffentlich zur Verfügung. Dazu gehören jedoch auch Daten, die man nicht gern für jedermann öffentlich abrufbar sehen möchte. Dazu solltet Ihr den vollständigen Artikel lesen, es gibt erstens noch viel mehr Informationen dazu und zweitens ein umfangreicheres Code-Beispiel.

Als kleines Goodie habe ich Dir noch ein Plugin geschrieben, das Du im Artikel herunterladen kannst.

WordPress REST-API Sicherheitslücke deaktivieren

Ein Code-Beispiel, das die REST-API für externe Besucher abschaltet

```
<?php
/* Ab hier kopieren */
/**
 * REST-API fuer extere User abschalten
 */
add_filter('rest_authentication_errors', function($result) {
if ( ! is_user_logged_in() ) {
return new WP_Error( 'rest_API_cannot_access', array( 'status'
=> rest_authorization_required_code() ) );
```

```
}
return $result;
});
```

PHP

Copy

WordPress absichern. Echte WordPress Sicherheit!

Du solltest die folgenden Arbeiten immer mit einem **FTP-Zugang** erledigen, niemals in den Editoren von WordPress. Diese gehören abgeschaltet, weil sie ein extremes Sicherheitsrisiko darstellen.

Wie das geht, erfährst Du weiter unten.

Die Snippets sind geeignet für:

- **WordPress-Version:** Ab 4.5 – inklusive 5.5.xx
- **PHP-Version:** inkl. PHP 7.4.xx

Am Ende dieses Artikels hast Du alle Sicherheitslücken geschlossen und kannst dich an einer sicheren Website erfreuen. Als spezialisierte SEO Agentur wissen wir, wovon wir sprechen. Wir führen Dich Schritt für Schritt durch die einzelnen Punkte.

Die Basis der Sicherheit. Eine perfekte .htaccess Datei

Seit mittlerweile 9 Jahren entwickle ich eine .htaccess Datei und habe sie jedes Jahr stets verbessert und überarbeitet. Sie ist die Grundlage einer guten Sicherheitsstrategie und sorgt zudem noch für einen enormen Performance-Schub für Dein WordPress.

Folgendes wird abgesichert:

- Alle wichtigen WordPress-Dateien und Ordner gegen Zugriff von außen
- Dank ausgeklügelter Firewall Schutz vor SQL-Injektionen
- Schutz gegen die Ausnutzung von eventuellen Sicherheitslücken in Plugins
- Schutz gegen die Einschleusung von Schadsoftware jeder Art
- Schutz gegen Brute-Force Angriffe auf Uploads-Ziele
- Setzt HTTP-Response Header für Browser-Sicherheit
- Sperrt die xmlrpc.php Datei gegen jeden Zugriff

Den Adminbereich von WordPress absichern

Der Adminbereich ist das Herz Deiner Website und sollte so sicher wie nur möglich sein. Das erreichen wir durch drei wichtige Schritte. Alle drei Maßnahmen sorgen dafür, dass sich Hacker die Zähne ausbeissen und keine Chance mehr haben, über diesen Weg in Deine Website einzudringen.

1

Teil 1: Eine zusätzliche Passwortabfrage – HTTP Authentifikation

Eine HTTP Authentifikation ist eine sehr wirkungsvolle Sache. Bevor man nicht die korrekten Zugangsdaten eingegeben hat, kommt man nicht an den Adminbereich von WordPress und kann sich demzufolge auch nicht einloggen. Diese zusätzliche Passwortabfrage ist schnell eingerichtet.

Du benötigst dafür **einen FTP-Zugang** zu Deinem Webhosting und ein **FTP-Programm** wie zum Beispiel FileZilla.

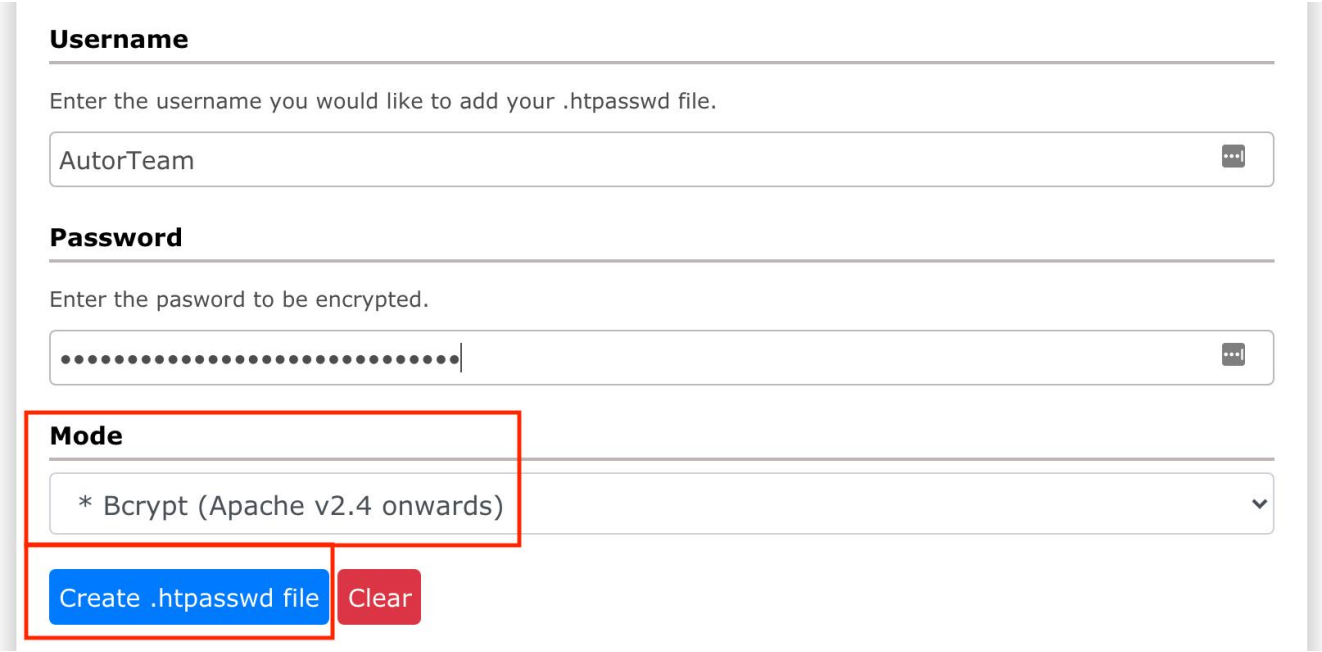
.htpasswd erstellen

Um diese Abfrage einzurichten benötigst Du erstens die obige .htaccess Datei und eine Datei namens .htpasswd, die Du erstellen musst. Beide Dateien sind versteckte – oder Systemdateien – die normalerweise nicht angezeigt werden. Du musst die Anzeige von versteckten Dateien also aktivieren.

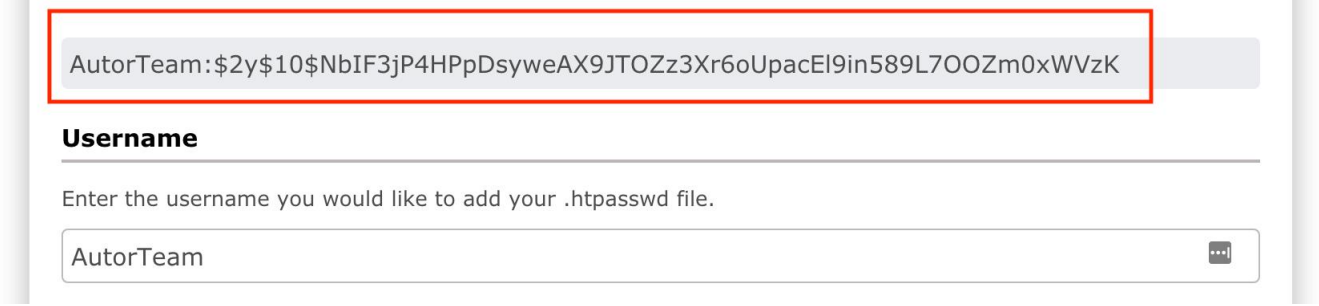
Lege nun mit dem Editor von Windows oder TextEdit von macOS eine reine Textdatei mit dem Namen .htpasswd an.

Erzeuge jetzt mit dem Passwort-Generator ein sicheres Passwort. Es sollte mindestens 25stellig sein. Notiere Dir das Passwort und rufe jetzt den .htpasswd Generator auf. Gib einen Benutzernamen Deiner Wahl ein und das soeben generierte Passwort.

Stelle bei »Mode« **Bcrypt** ein. Siehe Screenshot. Das sorgt für eine ziemlich gute Verschlüsselung des Passworts. Danach klicke auf den blauen Button.



Die dadurch erstellten Zugangsdaten findest Du oberhalb von Username.



Kopiere diese Zeile und füge sie in Deine .htpasswd Datei ein. Speichere die Datei ab und lade sie mit dem FTP-Programm in das Hauptverzeichnis von WordPress.

Jetzt muss der korrekte und vollständige Server-Pfad zur .htpasswd ermittelt werden.

Server-Pfad ermitteln

Um den vollständigen Server-Pfad zur Datei zu ermitteln, nutzen wir eine kleine PHP-Datei. Erstelle mit einem Text-Editor eine Datei namens dir.php und kopiere folgendes hinein:

```
<?php
$dir = dirname(__FILE__);
echo "<p>Der vollständige Pfad zur .htpasswd Datei in diesem Verzeichnis: " . $dir . "/.htpasswd" . "</p>";
```

PHP

Copy

Lade diese Datei nun in das Hauptverzeichnis von WordPress und rufe die Datei im Browser auf:

https://deine-website.de/dir.php

HTTP

Copy

Kopiere den angezeigten Pfad und notiere Ihn. Er sieht so aus:

```
 /usr/local/www/apache24/noexec/deinewebseite/.htpasswd
```

HTTP

Copy

Dieser Pfad muss nun in die .htaccess eingetragen werden. Wenn Du meine Datei nutzt, ist der betreffende Block relativ weit unten zu finden. Du musst vor dem Code die Rauten # entfernen, um ihn nutzen zu können.

So muss es nachher aussehen:

```
# ----------------------------------------------------------------------
#   Protect your WordPress Login with HTTP Authentification
# ----------------------------------------------------------------------

# If you want to use it, comment it out and set your path to .htpasswd
<Files wp-login.php>
 AuthName "Admin-Bereich"
 AuthType Basic
                                                AuthUserFile /usr/local/www/apache24/noexec/deinewebseite/.htpasswd
 require valid-user
</Files>
```

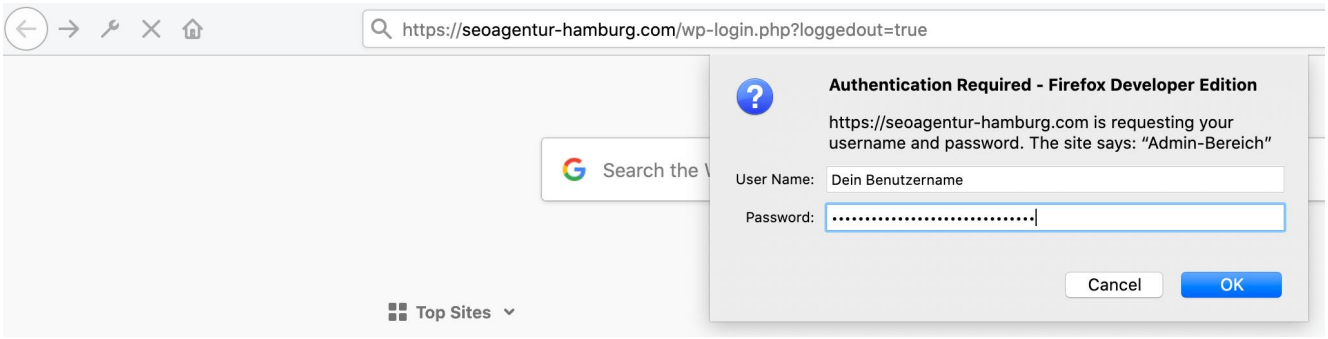
Apache Configuration

Copy

WICHTIG: Lösche jetzt die dir.php wieder vom Server. Sie stellt ein Sicherheitsrisiko dar.

Lade jetzt die .htaccess Datei wieder auf Deinen Server hoch. Jetzt sollten sich beide Dateien (.htaccess und .htpasswd) im Hauptverzeichnis von WordPress befinden.

Wenn Du jetzt Deinen Adminbereich aufrufst – egal ob mit wp-login.php oder wp-admin – kommt die folgende Passwortabfrage:



Übrigens musst Du die Zugangsdaten nur einmal eingeben, danach befindet sich die Abfrage im Browser-Cache. Erst wenn dieser gelöscht wird, kommt die Abfrage erneut.

2

Teil 2: WordPress absichern: Zugang nur noch mit E-Mail-Adresse

Ein kleines Code-Snippet mit großer Wirkung. Hacker probieren allen möglichen und unmöglichen Benutzernamen aus, bevorzugt natürlich »Admin«, weil er so weit verbreitet ist. Hat ein Hacker Deinen Benutzernamen, braucht er nur noch Dein Passwort.

Daher sorgen wir dafür, dass er garantiert nicht Deinen Benutzernamen bekommt. Weil es ihn nicht mehr gibt. Denn statt dem Benutzernamen kannst Du Dich nur noch mit Deiner E-Mail-Adresse und dem Passwort einloggen.

Kopiere den folgenden Code in die functions.php Deines (Child-) Themes. Du kannst für die Snippets auch ein eigenes Plugin anlegen.

```
<?php

// Ab hier kopieren

/**
 * Sicherheit: Anmeldung nur noch mit E-Mail-Adresse, anstatt Benutzernamen
 *
```

```
 * @author Andreas Hecht
 */

//WordPress Authentifikation löschen
remove_filter('authenticate',
'wp_authenticate_username_password', 20);

// Neue Authentifikation setzen - Anmelden nur mit E-Mail und
Passwort
add_filter('authenticate', function($user, $email, $password){

    //Check for empty fields
        if(empty($email) || empty ($password)){
            //create new error object and add errors to it.
            $error = new WP_Error();

            if(empty($email)){ //No email
                        $error->add('empty_username',
__('<strong>FEHLER</strong>: Das E-Mail Feld ist leer.'));
            }
                         else  if(!filter_var($email,
FILTER_VALIDATE_EMAIL)){ //Invalid Email
                       $error->add('invalid_username',
__('<strong>FEHLER</strong>:  Die  E-Mail-Adresse  ist
ungültig'));
            }

            if(empty($password)){ //No password
                        $error->add('empty_password',
__('<strong>FEHLER</strong>: Das Passwort-Feld ist leer.'));
            }

            return $error;
        }

        //Check if user exists in WordPress database
        $user = get_user_by('email', $email);

        //bad email
        if(!$user){
            $error = new WP_Error();
```

```
                                    $error->add('invalid',
__('<strong>FEHLER</strong>: Deine Eingaben sind ungültig.'));
            return $error;
        }
        else{ //check password
            if(!wp_check_password($password, $user->user_pass,
$user->ID)){ //bad password
                $error = new WP_Error();
                                    $error->add('invalid',
__('<strong>FEHLER</strong>: Deine Eingaben sind ungültig.'));
                return $error;
            }else{
                return $user; //passed
            }
        }
}, 20, 3);
```

PHP

Copy

3

Teil 3: Redirect auf Google nach falscher Eingabe der Zugangsdaten

Mit diesem Code-Snippet wirst Du garantiert jeden Hacker verblüffen, der es doch bis zum Adminbereich geschafft hat. Einmal die Zugangsdaten falsch eingegeben, und schon ist Google Dein bester Freund.

```
<?php

// Ab hier kopieren
if ( ! function_exists( 'ah_redirect_after_login_errors' ) ) :
/**
 * Redirect auf Google nach falscher Eingabe der WP-
Zugangsdaten
 */
function ah_redirect_after_login_errors() {
```

```
  wp_redirect( 'https://www.google.de' );
  exit;
}
add_filter( 'login_errors', 'ah_redirect_after_login_errors'
);
endif;
```

PHP

Copy

WordPress absichern mit den richtigen Einstellungen für die wp-config.php

Die wp-config.php Datei an sich haben wir ja schon mit der .htaccess abgesichert. Jetzt kommen noch wichtige Einstellungen in diese WordPress-Steuerungsdatei hinein.

Der korrekte Platz für unsere Eintragungen ist **oberhalb** der define('WP_DEBUG', false); Konstante.

1

Nutze die Sicherheitsschlüssel!

Die Sicherheitsschlüssel sorgen für eine Verschlüsselung Deiner Zugangsdaten während des Logins. Nutzt Du keine, werden die Zugangsdaten unverschlüsselt übertragen.

```
<?php


/**#@+
 * Sicherheitsschlüssel
 *
  * Ändere jeden untenstehenden Platzhaltertext in eine
beliebige,
 * möglichst einmalig genutzte Zeichenkette.
```

```
       *       Auf       der       Seite       {@link
https://api.wordpress.org/secret-key/1.1/salt/  WordPress.org
secret-key service}
 * kannst du dir alle Schlüssel generieren lassen.
 * Du kannst die Schlüssel jederzeit wieder ändern, alle
angemeldeten
 * Benutzer müssen sich danach erneut anmelden.
 *
 * @since 2.6.0
 */
define('AUTH_KEY',                                  ')tr/o
>x!>CD+@VV4EH}TAmm+i[!]f4|r.>K@MCo/,wDkBq^`c_0t9>fkgPnO?;g');
define('SECURE_AUTH_KEY',
'Zw!x0qEni%?OdHHs*s[kRF3ULD~xw*iCWO9F6oyzdL}}8%e2>+{Cd@a~`2>wQ
-S|');
define('LOGGED_IN_KEY',
'W<De;xTff~PE?^xXlE{vkN{O$mOlSIz`4za`cYk/;-
<<&/hC>a.Q1!k`mK>HE6bQ');
define('NONCE_KEY',                        'qH_9<.w&fC6$
YON~WK`zge#iuc3~<WPLD5nF;Bdl8:+G)2+s_vzk&bVC79C2>?b');
define('AUTH_SALT',
'X*2OOu?q)JhQ3=NUumf[(I^u?|sH|>vY?r^:XPJLW
+w7JCYeakqAjtjnI{_h~1a');
define('SECURE_AUTH_SALT',
'0wyeDI|N[]8}U<m[>g{]MhVA@WA|*<h}=j9i2vM)3m%`a/gtVSoH7>
mb|cN2VL/');
define('LOGGED_IN_SALT',                   'U]y/VEz<pP$-
+r0Iv^.CGBSh$.zI;~HSp:p0xtb9YMN%46${^F>?Bd!xrm$y}^bq');
define('NONCE_SALT',           '-|~?0 Hs%`,Ce$d+Oo#.mw
D5MW<7aI`Of]:gkp`r6S}tJfumjn2jvQsJqz-vgvM');
```

PHP

Copy

Die folgende Website generiert Dir die Schlüssel:

https://api.wordpress.org/secret-key/1.1/salt/

Schalte die Editoren für Theme und Plugins ab

> *In jeder WordPress-Installation kann man Theme- und Plugin-Dateien direkt im Adminbereich bearbeiten. Unter den Menüpunkten »Design« und »Plugins« findet man auch jeweils den Editor für die betreffenden Dateien. Dieser Editor ist sehr gefährlich, wenn er in die Hände eines Hackers gerät.*

```
<?php


/**
 *
 * Files Editoren abschalten
 *
 */
define('DISALLOW_FILE_EDIT', true);
```

PHP

Copy

3

Login in den Adminbereich nur über HTTPS

Sollte selbsterklärend sein. Wenn Deine Website HTTPS nutzt, sollte auch kein HTTP-Login in den Adminbereich möglich sein.

```
<?php

// Forciere das Anmelden mit SSL
define('FORCE_SSL_LOGIN', true);

// Adminbereich nur Nutzbar mit SSL
define('FORCE_SSL_ADMIN', true);
```

PHP

Copy

4

Datenübertragung nur mit FTPS

Die Datenübertragung von Deinem Rechner zum FTP-Zugang Deiner Website sollte ausschliesslich mit FTPS erfolgen. Tut es das nicht, werden Deine Zugangsdaten unverschlüsselt an den Server übertragen. Das wäre ein enormes Sicherheitsrisiko.

```
<?php

//FTP nur über SSL
define('FTP_SSL', true);
```

PHP

Copy

Extra: Du hast einen Blog mit mehreren Autoren?

Dann solltest du Deine Autoren daran hindern, einfache Passwörter zu verwenden. Hier kommt ein Code-Snippet, dass Deine Autoren daran hindert, ihre Passwörter zu ändern.

```
<?php

//Ab hier kopieren
/**
 * Sicherheit: User davon abhalten, ihre Passwörter zu ändern
 *
 * @author Andreas Hecht
 */
class Password_Reset_Removed
{
```

```
  function __construct()
  {
      add_filter( 'show_password_fields', array( $this,
'disable' ) );
      add_filter( 'allow_password_reset', array( $this,
'disable' ) );
  }

  function disable()
  {
    if ( is_admin() ) {
      $userdata = wp_get_current_user();
      $user = new WP_User($userdata->ID);
      if ( !empty( $user->roles ) && is_array( $user->roles )
&& $user->roles[0] == 'administrator' )
        return true;
    }
    return false;
  }

}

$pass_reset_removed = new Password_Reset_Removed();
```

PHP

Copy

Entfernen der XML-RPC Schnittstelle aus dem HTML-Header der Website

Die gefährliche Datei xmlrpc.php haben wir ja bereits mit der .htaccess Datei gesperrt, jetzt entfernen wir diese Schnittstelle noch aus dem HTTP-Response Header. Der Code kommt in die functions.php.

```
<?php

//Ab hier kopieren
if ( ! function_exists( 'AH_remove_x_pingback' ) ) :
/**
```

```
 * Entfernen der XML-RPC Schnittstelle aus dem HTML-Header der Website
 */

 function AH_remove_x_pingback( $headers )
 {
 unset( $headers['X-Pingback'] );
 return $headers;
 }
add_filter( 'wp_headers', 'AH_remove_x_pingback' );
endif;
```

PHP

Copy

Kleines FAQ zur WordPress Sicherheit

Bringt es was, wenn ich die wp-config.php verschiebe?

Nein. Außer das Du Deine Website fehleranfälliger gemacht hast nicht. Hacker finden die Datei, auch wenn Du sie verschiebst. Das bringt absolut nichts.

Was bringen Sicherheitsplugins wie WordFence, Sucuri etc.

Absolut nichts. Sie gaukeln Dir eine Sicherheit vor, die sie nicht erfüllen können. Diese Plugins versprechen Sicherheit, weil sie Deine WP-, Theme- und Plugin-Dateien auf Schadsoftware scannen. Wenn Du gehackt wurdest, manipuliert der Hacker zuerst diese Plugins. Denn er will ja, dass der Hack möglichst lange unentdeckt bleibt. Zudem sorgen diese

Plugins noch dafür, dass Deine Website deutlich langsamer wird. Wenn Du Sicherheit willst, dieser Artikel ist die Anleitung dazu.

Ich brauche keine WordPress Absicherung. Ich habe Limit Login Attemps!

Klasse. Ehrlich. Einen Hacker im ersten Lehrjahr kannst Du damit erschrecken. Profis werden vor Lachen auf dem Fußboden liegen. Warum? Das Plugin limitiert die Loginversuche von EINER bestimmten IP-Adresse. Profis hingegen greifen Dich mit einem Botnetz an. Da prasseln dann Tausende von Anfragen an Deinen Adminbereich von Tausenden von IP-Adressen ein. Wenn von jeder IP nur ein Hackversuch kommt, kann das Plugin nichts stoppen. Im Grunde ist es vollkommen wirkungslos.

Soll ich explizite Dateiberechtigungen auf dem Server setzen?

Hmm, kannst Du schon machen. Aber ob das wirklich praktikabel ist, ist die zweite Sache. Ab und an brauchen Plugins bestimmte Berechtigungen, um zu funktionieren. Auch Updates müssen ohne Probleme laufen. Natürlich kann man sagen, dass man durch Dateiberechtigungen die Manipulation der Dateien von Außen unterbindet.

Im Prinzip wäre das nützlich. Aber Du hast durch meine .htaccess ja schon den Zugriff auf die wichtigsten Dateien gesperrt. Wenn ich auf die Dateien nicht zugreifen kann, kann ich sie auch nicht manipulieren.

WordPress absichern durch das Abändern des Benutzernamens?

Auch erfahrene WordPress Webworker wie Perun empfehlen Dir, den Standard »Administrator« oder »Admin« in einen anderen Benutzernamen abzuändern. Manche gehen einen Schritt weiter

und empfehlen Dir, den ersten Admin zu löschen und vorher einen weiteren Admin mit eigenem Benutzernamen anzulegen, um die #ID 1 gegen eine #ID 2 auszutauschen.

Kann dieser Tipp meine Website sicherer machen?

Nein. Der Tipp zeugt von absolut fehlender Sachkenntnis oder von nicht durchdachter Problemstellung. Der Benutzername des Administrators kann innerhalb von Sekunden herausgefunden werden.

Denn jede Autor-Box unter den Beiträgen und jedes Autoren-Archiv in WordPress gibt den Benutzernamen preis. Solltest Du also mit einem Admin-Account Beiträge schreiben, geben alle zwei Möglichkeiten Deinen Admin-Benutzernamen preis.

Wenn alles nichts bringt, kann der Benutzername auch im Quelltext der Kommentare gefunden werden. Ups…

Zwei Beispiele:

https://gist.github.com/seoagentur-hamburg/c96bc796764baaa64d43b70731013f8a#file-htaccess

eine automatische Aktualisierung durchführen

„wp-config-php“ lässt sich durch den Eintrag

```
define( ‚WP_AUTO_UPDATE_CORE‘, true );
```

Plugins automatisch aktualisieren

```
add_filter( 'auto_update_plugin', '__return_true' );
```

Themes automatisch aktualisieren

```
add_filter( 'auto_update_theme', '__return_true' );
```

Du bist auf der Suche nach einer seriösen SEO Agentur?

Dir hat unser Artikel gefallen und Du möchtest unsere Hilfe in Anspruch nehmen? Dann melde dich bei unverbindlich bei uns. Wir freuen uns auf Deine Anfrage!

+49 40 – 209 659 47info@seoagentur-hamburg.com

Jetzt weitere interessante Beiträge lesen

WordPress

Google Fonts Download: Den Google Font lokal laden

vor 1 Jahr

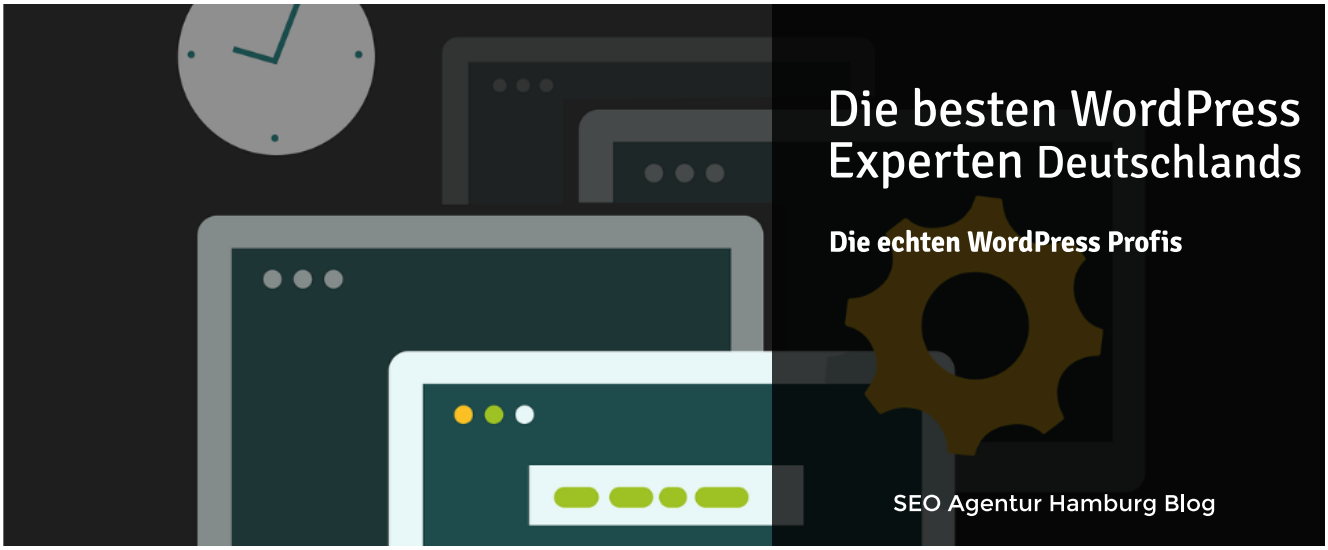
Google Schriften zu verwenden ist sehr beliebt. Doch ein Google Font verursacht erhebliche DSGVO Probleme, da Daten in die USA…

WordPress

Wie Du ein WordPress Child Theme erstellen kannst für Anfänger

vor 3 Jahren

Um zu vermeiden, dass ein Theme-Update eigene Änderungen überschreibt, lohnt es sich, ein WordPress-Child-Theme zu erstellen. Denn ein Child Theme…



WordPress

Die 10 besten WordPress Spezialisten Deutschlands?

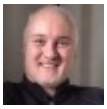
vor 4 Jahren

Ich wurde vor einiger Zeit im Rahmen einer Spezialistenempfehlung als einer der zehn besten WordPress Spezialisten Deutschlands von der Website…

39 Kommentare. Hinterlasse eine Antwort

- Markus16. Februar 2023 10:34 Hallo Andreas, nochmals herzlichen Dank für diese vielen Infos hier. Ich habe festgestellt, dass nach Entfernen der XML-RPC

Schnittstelle aus dem HTML-Header der Website die Seite nicht mehr erreichbar ist. Als ich den Eintrag aus der wp-config entfernt hatte, lief es wieder. Kennst du das Phänomen bzw. hast du eine Idee, woran es liegen könnte? Antworten

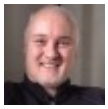
-  Andreas Hecht16. Februar 2023 14:32 Hi Markus,ich habe im Artikel nichts davon geschrieben, dass der Code zum Entfernen der XML-RPC Schnittstelle in die wp-config.php hinein soll. Lesen hilft in solchen Fällen ungemein. Antworten

-  Isa1. Februar 2023 19:39 Hallo Andreas,
Danke für diese Anleitung. Ich habe diese umgesetzt und alles Funktioniert bis auf eine Kleinigkeit: Ich benutze deine htaccess Datei und habe anschließend die zusätzliche Passwortabfrage (HTTP Authentifikation) mit reingenommen. Sobald ich mich anmelde komme ich rein, allerdings sobald ich den Browser neustarte muss ich die Daten erneut eingeben (die Login Daten speichern sich anscheinend nicht im Cache ab. Kann es sein das es was mit der htaccess Datei zu tun hat, da diese ja den Cache komprimiert? Den Cache vom Browser löschen hat nichts gebracht. Übrigens nutze ich All-Inkl als Hoster. Ich finde den Fehler nicht. Hast du da einen Tipp? Antworten

  -  Andreas Hecht1. Februar 2023 20:43 Hi Isa,das hört sich für mich an, als ob der Cache des Browsers beim beenden geleert wird. Antworten

    -  Isa4. Februar 2023 9:40 Danke für die Schnelle Antwort. Allerdings ist es nicht

nur auf einem Gerät und Browser so sondern bei allen die ich jetzt ausprobiert habe. Eine Lösung habe ich dazu noch nicht gefunden. Antworten

-  Frank19. September 2022 1:09 Toller Artikel! Funktionieren die Snippets auch mit WordPress 6.0.2. ? Antworten
  -  Andreas Hecht25. September 2022 15:11 Hallo Frank,ja, das tun sie. Antworten

-  Frank16. September 2022 1:28 I'm Snippet „REST-API fuer extere User abschalten" hat sich eine fehlerhafte Klammersetzung eingeschlichen.
„return $result;" wird nie ausgeführt und der Filter liefert demzufolge nichts zurück, wenn die Bedingung nicht zutrifft. Antworten
  -  Andreas Hecht16. September 2022 14:27 Hi Frank,bei meinem Test wird genau das gewünschte Ergebnis erreicht. Was genau sollte da nicht funktionieren? Antworten
    -  Frank19. September 2022 23:54 Hallo Andreas,also wenn du zweimal hintereinander ein „return" laufen lassen willst wie in deinem Beispiel oben, dann kann das 2. return doch nie erreicht werden, weil das erste return die gesamte Funktion verlässt

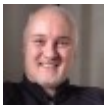
und alles danach schlicht nicht mehr ausgeführt wird.Die Funktion macht formal in folgender Form weitaus mehr Sinn:

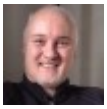
```
add_filter('rest_authentication_errors',
function($result) {
if ( ! is_user_logged_in() ) {
return new WP_Error(
'rest_API_cannot_access', array( 'status' =>
rest_authorization_required_code() ) );
}
return $result;
});
```

… und zwar darum, weil add_filter() sich von add_action() in WP dadurch unterscheidet, dass add_filter einen Wert entgegennimmt, ihn modifiziert (oder auch nicht) und dann wieder zurückgibt. Deine Funktion oben gibt aber praktisch immer dann gar nichts zurück, wenn die Bedingung nicht greift, also im konkreten Fall: wenn du eingeloggt bist. Ein eingeloggter Benutzer wird daher NIE eine REST-Error zu sehen bekommen, auch dann nicht, wenn es einen gibt. Mag schon sein, dass dann alles funktional erscheint, aber wenn Fehler, die auftreten, nicht rückgemeldet werden, muss noch lange nicht alles in Ordnung sein …
Ich hoffe, das hilft. Die Klammer ist einfach verrutscht – keine große Sache.
Antworten

-  Andreas Hecht25. September 2022 15:12 Hi Frank,okay, das hatte ich nicht bedacht. Danke für Deine Mühe,

ich ändere das Snippet ab. Antworten

-  Joachim2. September 2022 10:21 Hallo Andreas, ich hoffe, du kannst mir helfen: Es geht um Teil 1, eine zusätzliche Passwortabfrage. Die Schritte habe ich alle ausgeführt und die Eingabemaske erscheint auch bei mir. Allerdings geht es nach der Eingabe der Zugangsdaten nicht weiter, sondern die Maske erscheint einfach erneut und es geht nicht weiter. Verhindert eventuell die Ninja-Firewall die Ausführung? Ich würde mich freuen, wenn du helfen kannst. Mein Hoster ist All-Inkl. Antworten
  -  Andreas Hecht2. September 2022 14:14 Hi Joachim,schalte mal diese Firewall komplett ab. Diesen Mist brauchst Du nicht mehr. Wenn es dann noch nicht funktioniert, stimmt etwas mit dem Pfad zur .htpasswd nicht. Antworten

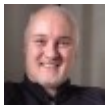
-  Heiko26. Mai 2022 10:04 Hallo Andreas, diese Seite wurde am 25.05.2022 aktualisiert, hat sich inhaltlich was geändert? Bei der Gelegenheit möchte ich mal DANKE sagen für das Know-How, das du hier kostenlos mit uns teilst. Antworten
  -  Andreas Hecht26. Mai 2022 15:11 Hallo Heiko,ja, da ist die Absicherung der WordPress REST-API dazugekommen. Ich habe das heute noch einmal deutlicher herausgestellt. Antworten

- Heiko7. Juni 2022 15:09 Hallo Andreas, ich habe die Absicherung der REST-API ausprobiert, sowohl per Code als auch mit deinem Plugin. In beiden Fällen kann ich keine Beiträge mehr bearbeiten – es erscheint nur eine weiße Seite… Theme TwentyTwenty mit Twentig… Antworten
  -  Andreas Hecht7. Juni 2022 15:19 Hi Heiko,dann ist eines Deiner Plugins schlecht programmiert und benötigt die (komplette) Schnittstelle. Da kann man am Code nichts ändern. Antworten
    - Frank21. September 2022 13:36 Doch, kann man. Man könnte den Fehler im Snippet beseitigen, so: https://www.kuketz-blog.de/wordpress-rest-api-unter-wordpress-4-7-deaktivieren/ (https://www.kuketz-blog.de/wordpress-rest-api-unter-wordpress-4-7-deaktivieren/)Das Snippet kursiert in unzählige Male in falsch abgeschriebener Fassung im Netz, sogar beim Kulturbanausen. Auf dieser Seite einmal mehr.
  - Frank21. September 2022 13:28 Hi Heiko, ich würde das REST-Snippet

einmal auf die folgende (richtige) Variante abändern und schauen, ob es damit geht (dennwenn du als authentifizierter Benutzer REST-Fehler hast, produziert das Snippet selbst Fehler, weil es keinen Rückgabewert hat):
https://www.kuketz-blog.de/wordpress-rest-api-unter-wordpress-4-7-deaktivieren/
(https://www.kuketz-blog.de/wordpress-rest-api-unter-wordpress-4-7-deaktivieren/)
Schöne Grüße! Antworten

-  Leon17. Mai 2021 8:29 Kann man die Einträge in der functions.php des Child-Themens nicht auch in ein gesondertes Plugin schieben? Antworten
-  die schreibmaus22. April 2021 13:04 hallo andreas,auf der suche nach weiteren sicherheits-features für wordpress im netz bin ich auf eine andere seite gestoßen: „https://kinsta.com/de/blog/wordpress-url-loggst/“. dort empfehlen sie unter anderem, mithilfe des wps hide plugins die normale url, unter der üblicherweise der login stattfindet, umzubiegen auf eine beliebig selbstgewählte url, die der angreifer nicht kennen kann. das plugin funktioniert soweit, allerdings natürlich nicht in kombination mit der zusätzlichen Passwortabfrage (HTTP Authentifikation), die du am anfang deines artikels beschreibst. frage an dich als

experten: würde es sich lohnen, die login-url zusätzlich zu „verbiegen“, um hackerangriffe weiter zu erschweren? könnte man das mit deiner zusätzlichen passwortabfrage kombinieren? vermutlich müsste man deine .htaccess-datei noch mal anpassen, aber dafür bin ich nicht profi genug. es wäre toll, wenn du das machen könntest, sofern du es für sinnvoll hältst.liebe grüße,die schreibmaus
Antworten

-  Andreas Hecht22. April 2021 13:12 Das verstecken der Login-URL hilft nicht, das können Hacker schnell herausfinden. Antworten

  -  die schreibmaus28. April 2021 13:53 vielen dank für deine einschätzung! Antworten

-  schreibmaus21. April 2021 19:53 hallo andreas,vielen dank für dein tolles tutorial! die beschriebenen dinge haben gut funktioniert, bis auf eines: der redirect auf die google-startseite bei eingabe eines falschen logins funktioniert bei mir so nicht. jedenfalls bekomme ich da genauso eine weiße seite mit wordpress-logo angezeigt, wir der andere andreas, der die schrieb. dabei bin ich kein anfänger und habe das gesamte tutorial bestimmt 5 mal gelesen. hast du eine idee, was ich eventuell doch falsch mache?danke dir für eine rückmeldung,
die schreibmaus Antworten

-  schreibmaus19. April 2021 20:59 hallo andreas,herzlichen dank auch von mir für diesen tollen

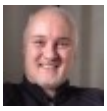
beitrag. was die weiterleitung zu google angeht, geht es mir allerdings wie dem anderen andreas hier, zitat:„Das mit dem Redirect beim falscher Eingabe der Zugangsdaten passt bei mir leider auch noch nicht. Statt Redirect bekomme ich eine leere Seite mit dem WP-Logo (befinde mich da noch immer auf meiner Domain).“das geht mir leider auch so. habe das snippet direkt nach dem „Anmeldung nur noch mit E-Mail-Adresse“-snippet am beginn der functions.php-datei des child-themes eingefügt. ich bin zwar kein anfänger, aber trotzdem unsicher, ob ich das entsprechend richtig gemacht habe, weil es – wie gesagt – nicht funktioniert.vielleicht hast du eine idee, was ich falsch mache.die schreibmaus
Antworten

-  Konstantin3. März 2021 15:33 Moin Moin,
kann sein das: Teil 3: Redirect auf Google nach falscher Eingabe der Zugangsdaten
mit dem aktuellen WordPress nicht mehr funktioniert?
Antworten

-  Frank15. Dezember 2020 17:25 Hallo Andreas,
einfach mal ein herzliches Dankeschön für deine tolle Arbeit, die unglaublich viel Zeit spart und WP deutlich sicherer macht. Bleib gesund und herzliche Grüße
Frank Antworten

-  Tilo10. Dezember 2020 16:37 Hallo,1.000 Dank für die hervorragende Anleitung.Ich habe ein paar Fragen und Probleme, die evtl. beantwortet und gelöst werden könnten.Zu Punkt Teil 2: WordPress absichern: Zugang nur noch mit E-Mail-Adresse:
Mit der Benutzeranmeldung (normale Kundenanmeldung) hinter einem woocommerceshop, können sich die Kunden nun auch alle nur noch mit der E-Mail anmelden? Oder gilt

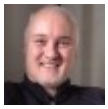
dies nur für den Admin?…lese ich am Code zumindest nicht heraus. Das würde evtl. für Probleme sorgen, da nicht alle Kunden so firm drinnen sind.Zu Punkt htaccess und Firewall:
ich habe seit der Umstellung auf die/Ihre htaccess auf experten-kredite.de Probleme mit dem PlugIn CalculateFiledsForm (Button „Direkt anfragen“). Da ich dort Daten abfrage und via Clickevent weitergebe denke ich das dies an einer Firewallregel liegt, da er mir im Anschluss einen 403 ausgibt.Gibt es dafür evtl. eine Lösung?Vielen Dank
Tilo Antworten

-  Andreas Hecht10. Dezember 2020 17:58 Hallo Tilo,Punkt 2: Ja, das dürfte sich auch auf die WooCommerce-User auswirken. Zur .htaccess: Der 403 sollte durch die 7G-Firewall ausgelöst werden. Da bitte die 7G-Firewall in der Datei gegen die 6G-Firewall austauschen. Siehe: https://seoagentur-hamburg.com/die-perfekte-htaccess-fuer-wordpress/ (https://seoagentur-hamburg.com/die-perfekte-htaccess-fuer-wordpress/) Antworten

  -  Tilo11. Dezember 2020 7:05 Hallo Andreas,Vielen Dank für deine schnelle Antwort…Mit der Anmeldung mit einem woocommerceshop gibt es da sicher einige Probleme mit Kunden, da ja da auch steht „Benutzername oder E-Mail-Adresse“ (hier mal am Kundenbeispiel https://viewegerback.de/mein-konto/ (https://viewegerback.de/mein-konto/)). Gibt der Nutzer nicht die/seine E-Mail ein, wird er auf Google weitergeleitet. Hier ist die Frage, an dich als Profi, ob es dafür

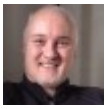
einen anderen Weg gibt. Einfachster Weg, die Zeile ändern in nur „E-Mail-Adresse“. Hier wäre die Frage, wo ich dies ändern muss?Mit der Firewall hatte ich die 6G getestet, aber da war gar nichts zu machen, sondern gleich alles dicht. Ich habe jetzt bei den Filtereinstellungen den einen Wert (null) rausgenommen…und es geht. Ich denke, das wird nicht gleich die Sicherheit auf den Kopf stellen. ;opDanke dir
Tilo Antworten

- 
  Tilo11. Dezember 2020 8:30
  …wichtig für alle die WordPress 5.6 und die .htaccess
  https://gist.github.com/seoagentur-hamburg/c96bc796764baaa64d43b70731013f8a#file-htaccess
  (https://gist.github.com/seoagentur-hamburg/c96bc796764baaa64d43b70731013f8a#file-htaccess)
  verwenden, sei noch mitgeteilt, dass die Permalinkstruktur evtl. neu gesetzt (wegen der Authorization) werden muss
  https://de.wordpress.org/support/topic/nach-update-auf-5-6-keine-bearbeitung-moeglich/
  (https://de.wordpress.org/support/topic/nach-update-auf-5-6-keine-bearbeitung-moeglich/) Antworten

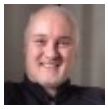
-  Iva29. Oktober 2020 15:21 Hallo Andreas,
vielen Dank für deinen hilfreichen Beitrag. Ich habe eine Frage noch: was würdest du empfehlen für die Absicherung der functions.php-Datei. Besonders sensibel sind z.B. die Zugangsdaten zu dem SMTP-Server, da Username und Passwort im Klartext stehen? Kann man sie verschlüsseln?
Besten Dank! Antworten
  -  Andreas Hecht13. November 2020 14:55 Sorry für die späte Antwort. Seit Corona habe ich mehr Arbeit als ich bewältigen kann. Warum willst Du einen E-Mail-Server (SMTP) in die functions.php eintragen? Antworten

-  Matthias28. Oktober 2020 3:06 Hey Andreas … interessanter Beitrag! Ich hab 2 Fragen.
1. Wenn ich das alles so umsetze, brauch ich dann noch Wordfence?
2. Das mit Child Theme hab ich nicht ganz verstanden .. Ich nutze kein Child Theme, kann ich dann das trotzdem anwenden? Danke Antworten
  -  Andi3. November 2020 0:20 Wenn du die 7G Firewall in deiner htaccess implementiert hast, ein 32 Zeichen langes Passwort und eine 2 Faktor-Authentifizierung, sowie zusätzlichen htacces-Schutz für wp-admin verwendest, dann brauchst du das Plugin „Wordfence“ nicht. Nutze am besten die htaccess-Datei, welche Adresse hier im Beitrag zur Verfügung stellt.Du könntest die von Andreas aufgeführten Anpassungen auch direkt in der

functions.php einfügen. Problem: Nach einem WordPress Update werden all deine Einträge überschrieben. Daher ist ein Child-Theme zu empfehlen.Andreas Hecht hat hier in seinem Blog eine Anleitung dazu. Antworten

-  Andreas2. September 2020 12:24 Hi Andreas,
toller Beitrag – aber gleich zwei Fragen.1) Umleitung auf Google nach falscher Eingabe der Zugangsdaten funktioniert bei mir nicht.
2) Login via E-Mails ist möglich, aber auch weiterhin mit dem Standard-Benutzernamen.Deinen Code habe ich in die funtions.php unter /wp-includes eingefügt. Ist das evtl. der Fehler? Oder muss ich deine Code Snippets direkt am Anfang oder am Ende der php-Datei einfügen? Antworten
  -  Andreas Hecht2. September 2020 12:31 Hi Andreas,genau deshalb schrieb ich, dass die Maßnahmen des Artikels nicht für Anfänger geeignet sind. Du kannst nicht einfach **irgendwo** etwas hinein kopieren und dann sagen, dass es nicht funktioniert. Der Code gehört in die functions.php **des verwendeten Themes!** Und da solltest Du vorher ein Child-Theme erstellt und aktiviert haben, ansonsten sind die Änderungen nach dem nächsten Theme-Update weg. Das steht da auch ganz deutlich, wo das hin muss. Man muss nur **LESEN**. Ich zitiere mich mal:Kopiere den folgenden Code in die functions.php Deines (Child-) Themes: Antworten
    -  Andreas2. September 2020 17:30 Trotzdem danke Andreas. Den Hinweis hatte ich auch gelesen, dachte mir aber, weil du

Child in Klammern gesetzt hast, dass es auch in die Haupt-Functions.php eingefügt werden kann. Sorry, Anfängerfehler.Aber wenn man als Anfänger keine Fragen stellt, kann sich an dem Status auch nichts ändern.
Und ich habe nicht behauptet, dass dein Code nicht funktioniert. Ich habe lediglich als Anfänger einen Fehler gemacht und hatte keine Erklärung dafür. Ich möchte ja den gesamten Code verstehen, bevor ich einfach nur ‚Copy and Paste' mache.Leider bin ich kein gelernter Informatiker und muss mir die Materie hier selbst erarbeiten und beibringen – nicht immer einfach.
Bevor ich Dir also weitere unnötige Fragen stelle, kannst du mir evtl. einen Tipp geben, welche Quellen ich für das Verstehen des Codes nutzen kann?Das mit dem Redirect beim falscher Eingabe der Zugangsdaten passt bei mir leider auch noch nicht. Statt Redirect bekomme ich eine leere Seite mit dem WP-Logo (befinde mich da noch immer auf meiner Domain). Entweder habe ich den Snippet an der falschen Stelle eingefügt (‚functions.php' im Hauptverzeichnis, da du hier ja nicht auf die functions.php des Child-Themes verwiesen hast oder?) oder es fehlt noch eine andere Voraussetzung, die ich übersehen habe.Deine Arbeit und Ratschläge weiß ich sehr wohl zu schätzen. Nochmals vielen Dank. Antworten

-  Andreas Hecht2. September 2020 17:55 Andreas,selbst wenn Du das (Child-) einfach mal streichst, bleibt noch »**in die functions.php Deines**

Themes« über. Dort, und nur dort kommt Code hinein. Und wenn Du willst, dass sich der Code auch noch nach einem Theme-Update dort befindet, dann erstellst Du von Deinem aktiven Theme ein Child-Theme, dass Du dann aktivierst. In dieses Child-Theme kommt ebenfalls eine functions.php hinein, in die dann jeder Code-Schnipsel hineinkommt. Übrigens muss man dafür kein Informatiker sein. Aber erstens sehr genau lesen und zweitens **VORHER fragen**, bevor man einfach irgendetwas macht, was man nicht versteht.

https://gist.github.com/seoagentur-hamburg/c96bc796764baaa64d43b70731013f8a#file-htaccess