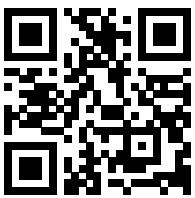
Der ultimative Leitfaden zur Sicherung von Kunden-Webseiten

KINSTA



Für die immer aktuelle Version scannen
Sie den obigen QR-Code oder gehen Sie zu
https://kinsta.com/de/ebooks/

Herausgegeben von KINSTA

Der ultimative Leitfaden zur Sicherung von Kunden-Webseiten

Inhalt

Der ultimative Leitfaden zur Sicherung von Kunden-Webseiten

Laut Internet Live Stats werden täglich über 100.000 Webseiten gehackt. 😮 Deshalb ist es so wichtig, sich etwas Zeit zu nehmen und die folgenden Empfehlungen durchzugehen, wie Sie die Sicherheit von WordPress verbessern können.

Wenn es um die Sicherheit von WordPress geht, gibt es viel mehr als nur die Sicherung Ihrer Webseite, obwohl wir Ihnen im Folgenden die besten Empfehlungen dazu geben werden.

Investieren Sie in sicheres WordPress-Hosting

Beginnen wir mit der Sicherheit auf Webserver-Ebene, für die Ihr WordPress Host verantwortlich ist. Es ist sehr wichtig, dass Sie einen Hoster wählen, dem Sie Ihr Business anvertrauen können, wenn Sie die Webseiten Ihrer Kunden auf diese übertragen.

Wenn Sie WordPress auf Ihrem eigenen VPS hosten, dann müssen Sie über die technischen Kenntnisse verfügen, um diese Dinge selbst zu tun. Aber um ehrlich zu sein, der Versuch, als Systemadministrator 20 Dollar/Monat zu sparen, ist keine effektive Art, ein Unternehmen zu führen.

Die Server-Härtung ist der Schlüssel zur Aufrechterhaltung einer durch und durch sicheren WordPress-Umgebung. Es sind mehrere Ebenen von Sicherheitsmaßnahmen auf Hardware- und Softwareebene erforderlich, um sicherzustellen, dass die IT-Infrastruktur, in der die WordPress-Seiten gehostet werden, in der Lage ist, anspruchsvolle Bedrohungen sowohl physischer als auch virtueller Art abzuwehren.

Aus diesem Grund sollten Server, auf denen WordPress gehostet wird, mit dem neuesten Betriebssystem und der neuesten (Sicherheits-)Software aktualisiert sowie gründlich auf Schwachstellen und Malware getestet und gescannt werden.

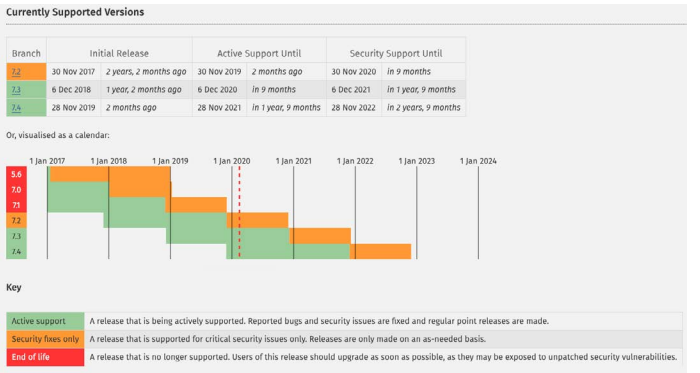
Firewalls auf Serverebene und Intrusion Detection Systeme sollten ebenfalls vorhanden sein, um die Webseiten Ihrer Kunden auch während der Installation von WordPress und der Erstellung der Webseite gut zu schützen. Die gesamte auf dem Rechner installierte Software zum Schutz von WordPress-Inhalten sollte jedoch mit den neuesten Datenbank-Management-Systemen kompatibel sein, um eine optimale Leistung zu gewährleisten. Der Server sollte auch so konfiguriert sein, dass er sichere Netzwerk- und Dateiübertragungsverschlüsselungsprotokolle (wie SFTP statt FTP) verwendet, um sensible Inhalte vor böswilligen Eindringlingen zu verbergen.

Wir nutzen die Google Cloud Platform hier bei Kinsta für alle unsere WordPress-Kunden, um ein sicheres WordPress Hosting zu gewährleisten. Die Sicherheit ist von Anfang an in unsere Architektur integriert und ist eine viel sicherere Methode als andere heute verfügbare.

Neueste PHP-Version verwenden

PHP ist das Rückgrat jeder WordPress-Seite, daher ist es sehr wichtig, dass die Webseiten Ihrer Kunden die neueste Version auf Ihrem Server verwenden. Jede größere Version von PHP wird in der Regel zwei Jahre lang nach ihrer Veröffentlichung voll unterstützt.

Während dieser Zeit werden regelmäßig Fehler und Sicherheitsprobleme behoben und gepatcht. Ab heute hat jeder, der mit der Version PHP 7.1 oder niedriger läuft, keinen Sicherheits-Support mehr und ist ungepatchten Sicherheitslücken ausgesetzt.



Currently Supported Versions

Branch	Initial Release		Active Support Until		Security Support Until	
7.2	30 Nov 2017	*2 years, 2 months ago*	30 Nov 2019	*2 months ago*	30 Nov 2020	*in 9 months*
7.3	6 Dec 2018	*1 year, 2 months ago*	6 Dec 2020	*in 9 months*	6 Dec 2021	*in 1 year, 9 months*
7.4	28 Nov 2019	*2 months ago*	28 Nov 2021	*in 1 year, 9 months*	28 Nov 2022	*in 2 years, 9 months*

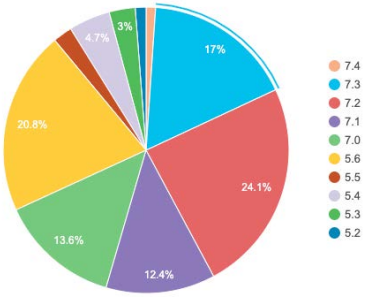
Or, visualised as a calendar:

Key

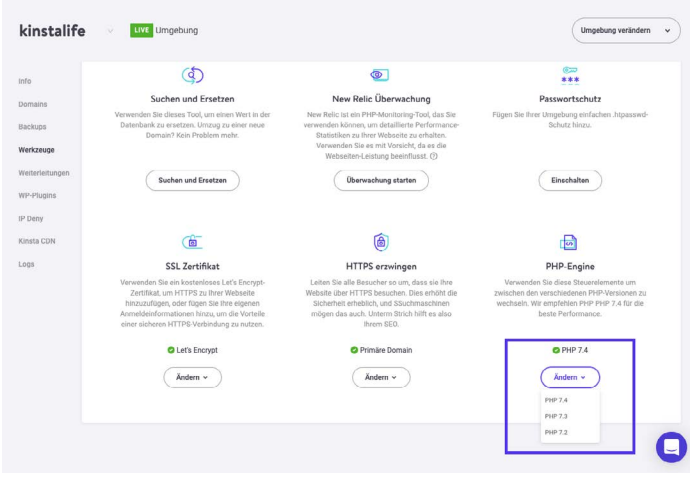
Active support	A release that is being actively supported. Reported bugs and security issues are fixed and regular point releases are made.
Security fixes only	A release that is supported for critical security issues only. Releases are only made on an as-needed basis.
End of life	A release that is no longer supported. Users of this release should upgrade as soon as possible, as they may be exposed to unpatched security vulnerabilities.

Und wissen Sie was? Laut der offiziellen WordPress Stats-Seite sind etwa 34% der WordPress-Benutzer immer noch mit PHP 5.6 oder niedriger ausgestattet, was bedeutet, dass mehr als ein Drittel der Benutzer derzeit PHP-Versionen verwendet, die nicht mehr unterstützt werden. Das ist beängstigend!

PHP Versionen



Hier bei Kinsta empfehlen wir nur die Verwendung von stabilen und unterstützten Versionen von PHP, einschließlich 7.2, 7.3 und 7.4. PHP 5.6, 7.0 und 7.1 sind ausgelaufen. Sie können sogar mit einem Klick auf eine Schaltfläche im MyKinsta-Dashboard zwischen den PHP-Versionen wechseln.



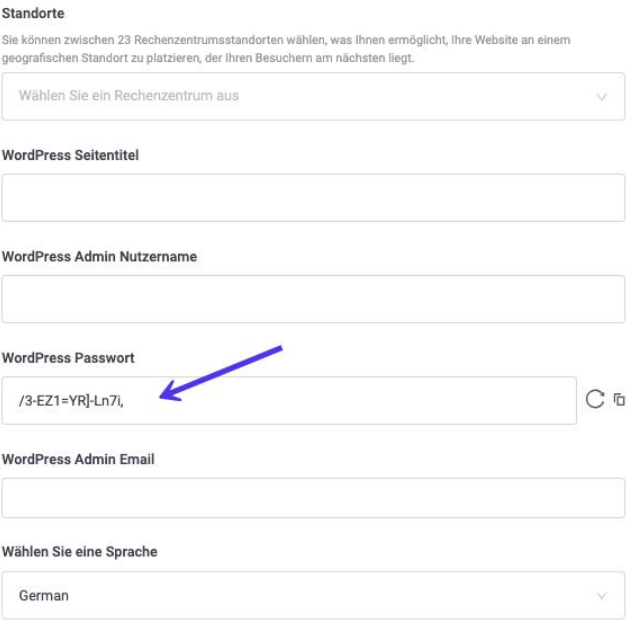
Wenn Sie es selbst ausprobieren wollen, gehen Sie einfach auf demo.kinsta.com und probieren Sie es aus! 

Verwenden Sie clevere Benutzernamen und Passwörter

Überraschenderweise ist eine der besten Möglichkeiten, die Sicherheit von WordPress zu erhöhen, die einfache Verwendung von cleveren Benutzernamen und Passwörtern. Klingt ziemlich einfach, oder? Schauen Sie sich die jährliche Liste 2019 von SplashData an, die die beliebtesten Passwörter, die im Laufe des Jahres gestohlen werden, auflistet (sortiert nach ihrer Beliebtheit).

- 123456
- 123456789
- qwerty
- password
- 1234567
- 12345678
- 12345
- iloveyou
- 111111
- 123123

Das beliebteste Passwort ist “123456”. Das ist ein Grund, warum wir hier bei Kinsta bei neuen WordPress-Installationen tatsächlich ein komplexes Passwort für die wp-admin-Anmeldung Ihrer Kunden erzwingen (wie unten auf unserem Ein-Klick-Installationsprozess zu sehen ist). Dies ist nicht optional.



Schauen Sie sich diese Funktion mit der MyKinsta-Demo an.

Die Kernfunktion wp_hash_password von WordPress verwendet das phpass-Passwort-Hashing-Framework und acht Durchläufe des MD5-basierten Hashings. Und was Ihre WordPress-Installation betrifft, sollten Sie auf den Webseiten Ihrer Kunden niemals den Standard-Benutzernamen “admin” verwenden, sondern vielmehr eindeutige WordPress-Benutzernamen für deren Administratorkonten erstellen.

Es ist auch wichtig, für jede Kundenseite unterschiedliche Passwörter zu verwenden. Am besten speichern Sie sie lokal in einer verschlüsselten Datenbank auf Ihrem Computer.

Ein gutes, kostenloses Werkzeug dafür ist KeePass. Wenn Sie diesen Weg nicht gehen wollen, gibt es auch Online-Passwortmanager wie 1Password oder LastPass.

Verwenden Sie immer die neueste Version von WordPress, Plugins und Themes

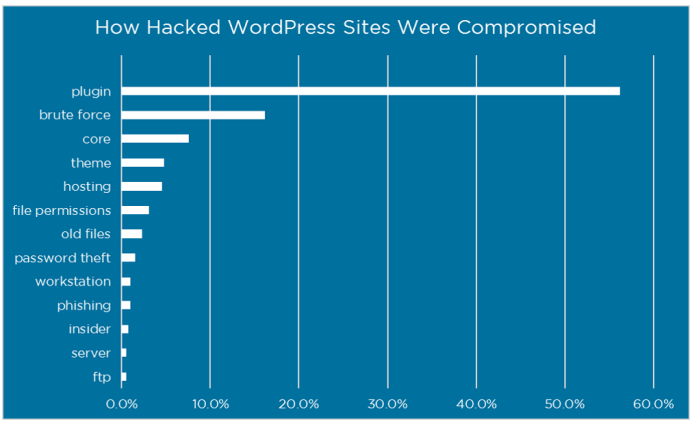
Eine weitere sehr wichtige Möglichkeit, die Sicherheit der Webseiten Ihrer Kunden zu erhöhen, besteht darin, sie immer auf dem neuesten Stand zu halten. Dies umfasst den WordPress-Core, Plugins und Themes. Diese werden aus gutem Grund aktualisiert, und oft beinhalten sie Sicherheitsverbesserungen und Fehlerbehebungen.

Leider gibt es Millionen von Unternehmen, die veraltete Versionen von WordPress-Software und Plugins einsetzen und immer noch glauben, dass sie auf dem richtigen Weg zum geschäftlichen Erfolg sind. Sie führen Gründe für die Nichtaktualisierung an, wie z.B. “Ihre Webseite wird kaputtgehen” oder “Coremodifikationen werden weg

sein" oder "Plugin X wird nicht funktionieren" oder "Sie brauchen die neue Funktionalität einfach nicht".

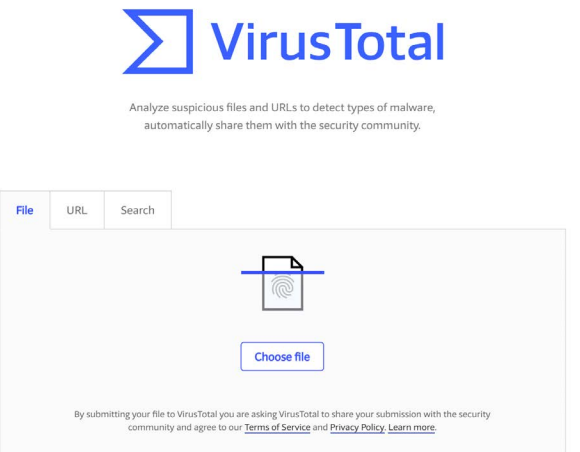
Tatsächlich gehen Webseiten meist aufgrund von Fehlern in älteren WordPress-Versionen kaputt. Coremodifikationen werden niemals vom WordPress-Team und von erfahrenen Entwicklern empfohlen, die die damit verbundenen Risiken verstehen. Und WordPress-Updates enthalten meist die notwendigen Sicherheitspatches sowie die zusätzlichen Funktionen, die für die Ausführung der neuesten Plugins erforderlich sind.

Wussten Sie, dass Berichten zufolge 55,9 % der bekannten Einstiegspunkte für Hacker auf Plugin-Schwachstellen zurückzuführen sind? Das fand WordFence in einer Studie, in der sie über 1.000 WordPress-Seiten-Betreiber befragten, die Opfer von Angriffen geworden waren. Durch die Aktualisierung Ihrer Plugins können Sie besser sicherstellen, dass Sie nicht zu diesen Opfern gehören.



Es wird auch empfohlen, nur vertrauenswürdige Plugins für Ihre Kunden zu installieren. Die Kategorien “Featured” und “Popular” im WordPress Repository können ein guter Ausgangspunkt sein. Oder laden Sie sie direkt von der Webseite des Entwicklers herunter. Wir raten dringend von der Verwendung von ungültigen WordPress-Plugins und -Themes ab.

Sie können ein Online-Tool wie VirusTotal verwenden, um die Dateien eines Plugins oder Themes zu überprüfen, um zu sehen, ob es irgendeine Art von Malware entdeckt.



Es gibt auch eine Menge Ressourcen, die Ihnen helfen, immer auf dem neuesten Stand der WordPress-Sicherheitsupdates und -Schwachstellen zu bleiben. Einige davon sind unten aufgeführt:

- WP Security Bloggers: Eine großartige aggregierte Ressource mit mehr als 20 Sicherheits-Feeds.

- WPScan Vulnerability Database: Kataloge mit über 10.000 WordPress Core, Plugin und Theme Schwachstellen.
- ThreatPress: Täglich aktualisierte Datenbank mit WordPress-Plugins, Themes und WordPress-Kern-Schwachstellen.
- Offizielles WordPress-Sicherheitsarchiv

Sperren Sie Ihren WordPress Adminbereich

Manchmal ist eine beliebte Strategie der WordPress-Sicherheit durch das Schaffen von Unklarheit für ein durchschnittliches Online-Geschäft und eine WordPress-Seite angemessen effektiv. Wenn Sie es für Hacker schwieriger machen, bestimmte Hintertüren zu finden, dann ist die Wahrscheinlichkeit eines Angriffs geringer. Das Sperren des WordPress-Adminbereichs und des Logins ist eine gute Möglichkeit, die Sicherheit zu erhöhen. Zwei großartige Möglichkeiten, dies zu tun, sind erstens die Änderung Ihrer Standard-WP-Admin-Login-URL und die Einschränkung von Login-Versuchen.

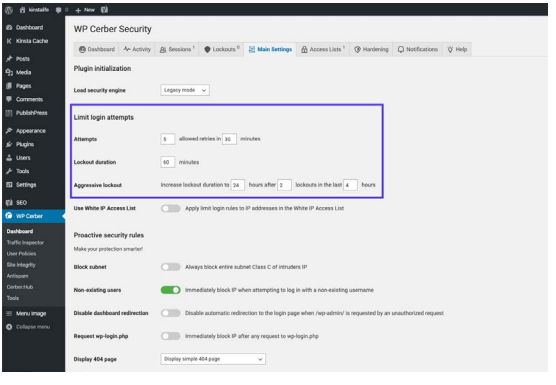
Wie Sie Ihre WordPress-Anmelde-URL ändern können

Standardmäßig lautet die Anmelde-URL Ihrer WordPress-Site domain.com/wp-admin. Eines der Probleme dabei ist, dass alle Bots, Hacker und Skripte da draußen dies auch wissen. Wenn Sie die URL ändern, können Sie sich weniger zur Zielscheibe machen und sich besser vor Brute-Force-Angriffen schützen. Dies ist kein Allheilmittel, sondern nur ein kleiner Trick, der Sie definitiv schützen kann.

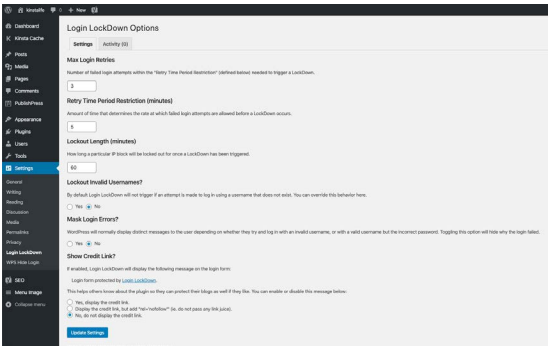
Um Ihre WordPress-Anmelde-URL zu ändern, empfehlen wir die Verwendung des kostenlosen WPS Hide Login-Plugins. Denken Sie einfach daran, etwas Einzigartiges auszuwählen, das nicht bereits auf einer Liste steht, die ein Bot oder ein Skript zu scannen versuchen könnte.

Wie man Login-Versuche einschränkt

Während die obige Lösung der Änderung Ihrer Admin-Login-URL dazu beitragen kann, die Mehrzahl der schlechten Login-Versuche zu verringern, kann die Festlegung einer Grenze auch sehr effektiv sein. Das kostenlose Plugin Cerber Limit Login Attempts ist eine großartige Möglichkeit, Sperrdauern, Anmeldeversuche sowie IP-Whitelists und -Blacklists einfach einzurichten.



Wenn Sie nach einer einfacheren Sicherheitslösung für WordPress suchen, ist eine weitere großartige Alternative das kostenlose Login Lockdown Plugin.

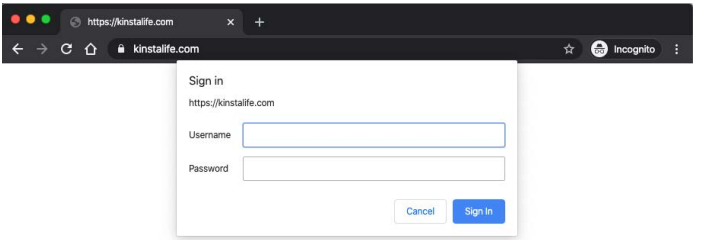


Login LockDown zeichnet die IP-Adresse und den Zeitstempel jedes fehlgeschlagenen Login-Versuchs auf. Wenn mehr als eine bestimmte Anzahl von Versuchen innerhalb eines kurzen Zeitraums aus demselben IP-Bereich erkannt wird, wird die Anmeldefunktion für alle Anfragen aus diesem Bereich deaktiviert. Und sie ist vollständig kompatibel mit dem oben erwähnten WPS Hide Login-Plugin.

Wenn Sie die Webseite Ihrer Kunden auf Kinsta umstellen, brauchen Sie kein zusätzliches Plugin für unsere Plattform zu installieren, denn sie begrenzt und blockiert böswillige Versuche automatisch.

Hinzufügen einer einfachen HTTP-Authentifizierung (htpasswd-Schutz)

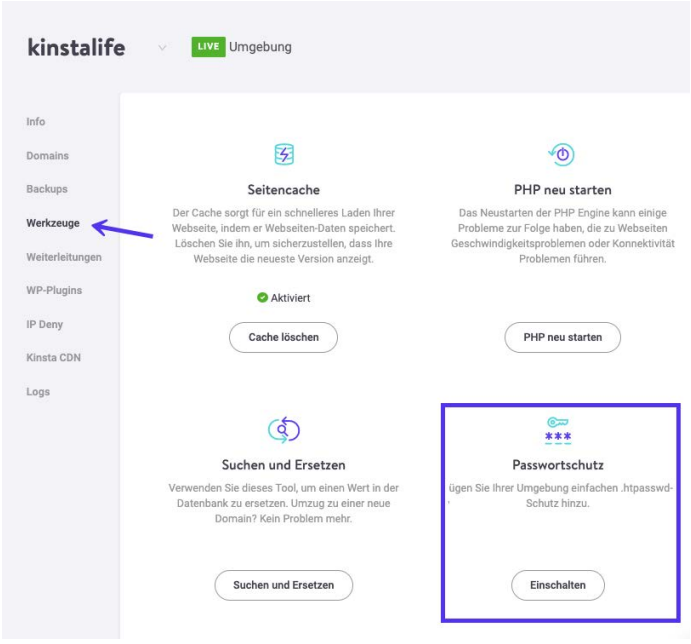
Eine weitere Möglichkeit, Ihren Admin-Bereich zu sperren, ist das Hinzufügen der HTTP-Authentifizierung. Dies erfordert einen Benutzernamen und ein Passwort, bevor Sie überhaupt auf die WordPress-Anmeldeseite zugreifen können.



Schauen Sie sich diese Funktion mit der MyKinsta-Demo an.

Wichtig: Dies sollte im Allgemeinen nicht auf eCommerce-Seiten oder Mitglieder-Webseiten verwendet werden. Aber es kann ein sehr effektiver Weg sein, um Bots daran zu hindern, Ihre Webseite zu besuchen.

Wenn Sie die Webseiten Ihrer Kunden bei Kinsta hosten, können Sie unser einfaches Passwortschutz-Tool (htpasswd) im MyKinsta-Dashboard verwenden (sehen Sie es in Aktion auf dem kostenlosen MyKinsta-Demokonto). Sie finden es unter der Rubrik “Tools” auf Ihrer Webseite. Klicken Sie einfach auf “Aktivieren”, wählen Sie einen Benutzernamen und ein Passwort, und schon können Sie loslegen!



Schauen Sie sich diese Funktion mit der MyKinsta-Demo an.

Nachdem sie aktiviert wurde, benötigt jede WordPress-Seite eine Authentifizierung, um auf sie zuzugreifen. Sie können die Anmeldedaten jederzeit ändern oder deaktivieren, wenn Sie sie nicht mehr benötigen.

Nutzen Sie die Vorteile der Zwei-Faktor-Authentifizierung (2FA)

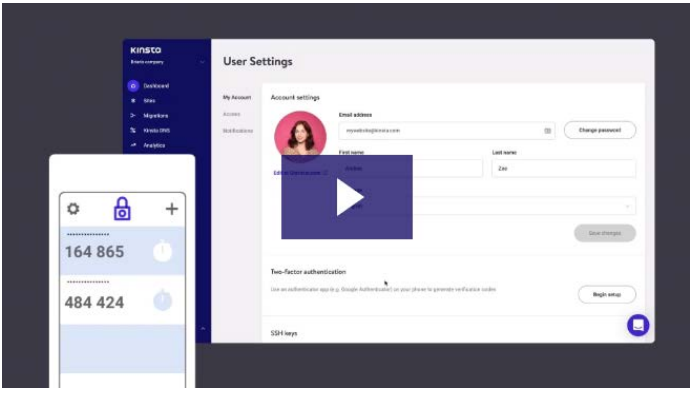
Die Zwei-Faktor-Authentifizierung umfasst einen zweistufigen Prozess, bei dem Sie nicht nur Ihr Passwort zur Anmeldung benötigen, sondern auch eine zweite Methode zur Anmeldung. In den meisten Fällen ist dies zu 100% effektiv, um Brute-Force-Angriffe auf die WordPress-Seiten Ihrer Kunden zu verhindern.

Es gibt jedoch zwei Teile, wenn es um die Zwei-Faktor-Authentifizierung für Kundenwebseiten geht.

Das erste ist Ihr Account und/oder das Dashboard, das Sie bei Ihrem Webhosting-Provider haben. Wenn jemand Zugang dazu erhält, könnte er die Passwörter aller Ihrer Kunden ändern, ihre Webseiten löschen, DNS-Einträge ändern und alle möglichen schrecklichen Dinge. Wir hier bei Kinsta verwenden für Ihr MyKinsta-Dashboard 2FA auf der Basis von Authenticator, weil:

- Das authentifizierungsbasierte 2FA ist sicherer als das SMS-basierte 2FA, da es nicht an Ihre Mobiltelefonnummer gebunden ist und nicht auf herkömmliche SMS-Technologie zurückgreift. Dadurch ist das authentifizierungsbasierte 2FA resistent gegen SIM-Swapping-Techniken.
- Das authentifizierungsbasierte 2FA kann für zusätzlichen Komfort mit Passwort-Manager-Anwendungen wie 1Password verwendet werden. Wenn Sie Ihre 2FA-Details zu einem Passwortmanager hinzufügen, müssen Sie sich nicht mehr auf ein externes Gerät verlassen um sich bei MyKinsta anzumelden.

Hier sehen Sie, wie einfach es ist, es zu aktivieren:



Der zweite Teil der Zwei-Faktor-Authentifizierung bezieht sich auf die tatsächlichen WordPress-Installationen Ihrer Kunden. Für diese gibt es ein paar Plugins, die Sie vielleicht testen und empfehlen möchten:

- Duo Zwei-Faktor-Authentifizierung
- Google Authenticator
- Two-Factor-Authentication

Nach der Installation und Konfiguration eines der oben genannten Plugins auf einer Kundenseite haben diese in der Regel ein zusätzliches Feld auf ihrer WordPress-Anmeldeseite, in das sie ihren Sicherheitscode eingeben können. Oder sie melden sich mit dem Duo-Plugin zunächst mit ihren Zugangsdaten an und müssen dann eine Authentifizierungsmethode wählen, wie z.B. Duo-Push, Anruf oder Passcode.

HTTPS für verschlüsselte Verbindungen verwenden - SSL-Zertifikat

Eine der am meisten übersehenen Möglichkeiten, die Sicherheit von WordPress zu erhöhen, ist die Installation eines SSL-Zertifikats und die Ausführung von Webseiten über HTTPS. HTTPS (Hypertext Transfer Protocol Secure) ist ein Mechanismus, der es jedem Browser oder jeder Webanwendung ermöglicht, eine sichere Verbindung mit einer Webseite herzustellen. Ein großes Missverständnis ist, dass die Webseiten Ihrer Kunden, die keine Kreditkarten akzeptieren, kein SSL benötigen.

Nun, lassen Sie uns ein paar Gründe erklären, warum HTTPS über den eCommerce hinaus wichtig ist. Viele Hosts, einschließlich Kinsta, bieten kostenlose SSL-Zertifikate von Let's Encrypt an.

6 Hauptgründe, warum HTTPS nicht nur für den eCommerce wichtig ist

1. Zusätzliche Sicherheit
Wie wichtig sind die Login-Informationen Ihrer Kunden? Nun, Sie sollten wissen, dass jedes Mal, wenn sich ein Benutzer einloggt, diese Informationen im Klartext an den Server übermittelt werden. HTTPS ist absolut unerlässlich, um eine sichere Verbindung zwischen einer Webseite und einem Browser aufrechtzuerhalten. Auf diese Weise können Sie Hackern und/oder einem Mittelsmann den Zugang zu den Webseiten Ihrer Kunden besser verhindern.

2. SEO
Google hat offiziell gesagt, dass HTTPS ein Ranking-Faktor ist. Da die meisten Ihrer Kunden wahrscheinlich jeden möglichen Vorteil

von SEO und SERPs nutzen würden, um ihre Konkurrenten zu schlagen, ist dies ein Kinderspiel.

3. Vertrauen und Glaubwürdigkeit
Laut einer Umfrage von GlobalSign suchen 28,9% der Besucher nach der grünen Adressleiste in ihrem Browser und 77% von ihnen sind besorgt darüber, dass ihre Daten online abgefangen oder missbraucht werden. Wenn sie dieses grüne Vorhängeschloss sehen, werden die Kunden sofort mehr Sicherheit haben, da sie wissen, dass ihre Daten sicherer sind.

4. Referral-Daten
Viele Leute wissen nicht, dass HTTPS-zu-HTTP-Referraldaten in Google Analytics blockiert werden. Was passiert also mit den Daten? Nun, das meiste davon wird einfach in den Abschnitt "direct Traffic" in einen Topf geworfen. Wenn jemand von HTTP zu HTTPS geht, wird der Referrer immer noch übergangen.

5. Chrome-Warnungen
Seit dem 24. Juli 2018 werden ab den Versionen von Chrome 68 und höher alle Nicht-HTTPS-Seiten als "Nicht sicher" gekennzeichnet, und ab 2020 begann der beliebte Browser, die Unterstützung für ältere TLS-Versionen zu verwerfen. Google macht den Besuchern viel deutlicher, dass eine WordPress-Webseite möglicherweise nicht auf einer gesicherten Verbindung läuft. Deshalb ist HTTPS wichtiger denn je!

6. Leistung
Aufgrund eines Protokolls namens HTTP/2 können diejenigen, die ordnungsgemäß optimierte Seiten über HTTPS betreiben, oft sogar Geschwindigkeitsverbesserungen feststellen.

HTTP/2 erfordert HTTPS wegen der Browser-Unterstützung. Die Leistungsverbesserung ist auf eine Reihe von Gründen zurückzuführen, wie z. B. die bessere Unterstützung von HTTP/2 für Multiplexing, Parallelität, HPACK-Komprimierung mit Huffman-Kodierung, die ALPN-Erweiterung und Server-Push.

Und mit TLS 1.3 sind HTTPS-Verbindungen noch schneller. Kinsta unterstützt TLS 1.3 auf allen unseren Servern und unserem Kinsta CDN.

Schauen Sie sich unseren ausführlichen WordPress HTTPS-Migrationshandbuch an, damit Sie besser werden, und erfahren Sie mehr in unserem TLS vs. SSL-Vergleich.

XML-RPC deaktivieren

In den letzten Jahren ist XML-RPC zu einem immer größeren Ziel für Brute-Force-Angriffe geworden. Es gibt ein paar WordPress-Plugins wie Jetpack, die auf XML-RPC angewiesen sind, aber die Mehrheit der Leute da draußen wird dies nicht brauchen, und es kann vorteilhaft sein, den Zugriff darauf einfach zu deaktivieren.

Wenn Sie hier bei Kinsta Kunde sind, brauchen Sie sich darüber keine Sorgen zu machen, da wir aktive und passive Maßnahmen ergriffen haben, um Angriffe und böswillige Absichten zu unterbinden. Insbesondere wird bei der Erkennung eines Angriffs über XML-RPC ein kleiner Codeschnipsel in die Nginx-Konfigurationsdatei eingefügt, um die Erzeugung eines 403-Fehlers zu verhindern.

Neueste HTTP-Sicherheitsheader hinzufügen

Ein weiterer Schritt, den Sie unternehmen können, um die Sicherheit Ihres WordPress-Clients zu erhöhen, ist die Nutzung von HTTP-Sicherheitsheadern. Diese werden normalerweise auf Webserver-Ebene konfiguriert und teilen dem Browser mit, wie er sich beim Umgang mit den Inhalten Ihrer Kundenseiten verhalten soll. Es gibt viele verschiedene HTTP-Sicherheitsheader, aber unten sind normalerweise die wichtigsten.

- Content-Security Policy
- X-XSS-Protection
- Strict-Transport-Security
- X-Frame-Options
- Public-Key-Pins
- X-Content-Type

Sie können überprüfen, welche Header derzeit bei jeder WordPress-Installation ausgeführt werden, indem Sie die Chrome-Devtools starten und sich den Header in der ersten Antwort Ihrer Webseite ansehen.

Hier ist ein Beispiel auf kinstalife.com (eine Demoseite). Sie können sehen, dass wir die x-content-type-options Header verwenden.

Wenn es um Kundenseiten geht, werden, wie im gezeigten Beispiel, standardmäßig immer x-content-type-options hinzugefügt, während x-frame-options und strict transport security nur bei Bedarf eingestellt werden.

Wenn Sie die Webseiten Ihrer Kunden scannen müssen, können Sie das mit dem kostenlosen Tool securityheaders.io von Scott Helme tun.

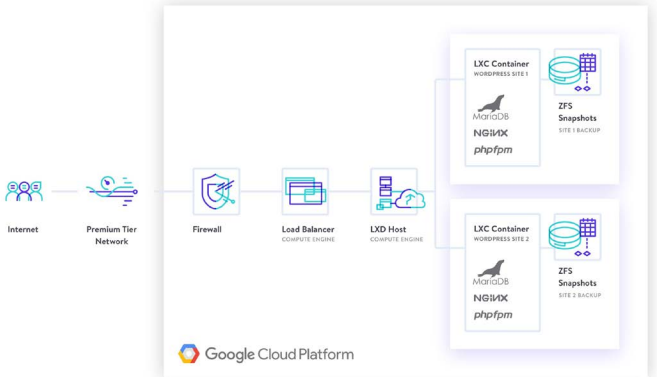
Es ist auch wichtig, sich bei der Implementierung von HTTP-Sicherheitsheadern daran zu erinnern, wie sich dies auf Ihre WordPress-Subdomains auswirken könnte. Wenn Sie z.B. den Content Security Policy-Header hinzufügen und den Zugriff nach Domains einschränken, müssen Sie auch Ihre eigenen Subdomains hinzufügen. Wenn Sie sich nicht sicher sind, wie Sie sie implementieren können, können Sie immer Ihren Host fragen, ob er Ihnen helfen kann.

WordPress-Sicherheits-Plugins verwenden

Es gibt eine Menge großartiger Entwickler und Unternehmen, die großartige Lösungen anbieten, um Ihre WordPress-Seite besser zu schützen. Nennenswerte sind:

- Sucuri Security
- iThemes Security
- Wordfence Security
- WP Security Audit Log
- WP fail2ban
- All In One WP Security & Firewall
- SecuPress
- BulletProof Security

- VaultPress
- Google Authenticator – Two Factor Authentication
- Security Ninja
- Defender
- Astra Web Security
- Shield Security
- Hide my WP
- WebARX



Kinsta verfügt über Hardware-Firewalls, aktive und passive Sicherheit, minutengenaue Verfügbarkeitsprüfungen und zahlreiche andere fortschrittliche Funktionen, um Angreifer am Zugriff auf Ihre Daten zu hindern. Wenn Ihre Webseite trotz unserer Bemühungen gefährdet ist, reparieren wir sie kostenlos.

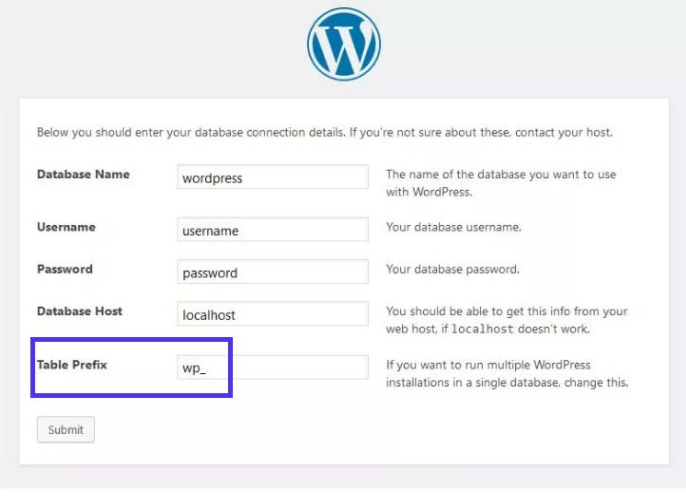
Eine sehr wichtige Funktion, die viele Sicherheits-Plugins enthalten, ist ein Prüfsummen-Dienstprogramm. Dies bedeutet, dass sie jede WordPress-Installation Ihres Kunden überprüfen und nach Änderungen an den Coredateien suchen, die von WordPress.org

(über die API) bereitgestellt werden. Änderungen oder Modifikationen an diesen Dateien können auf einen Hack hinweisen.

Sie können WP-CLI auch verwenden, um Ihre eigene Prüfsumme auszuführen. Schauen Sie sich diese zusätzlichen WordPress-Sicherheits-Plugins an, die helfen können, die „bösen Jungs“ auszuschließen.

Datenbank Sicherheit verbessern

Es gibt mehrere Möglichkeiten, die Sicherheit Ihrer WordPress-Datenbank zu verbessern. Die erste ist die Verwendung eines cleveren Datenbanknamens. Wenn Sie Ihren Datenbanknamen in einen etwas obskureren Namen ändern, hilft das, Ihre Webseite zu schützen, indem es Hackern die Identifizierung und den Zugriff auf Ihre Datenbankdaten erschwert.

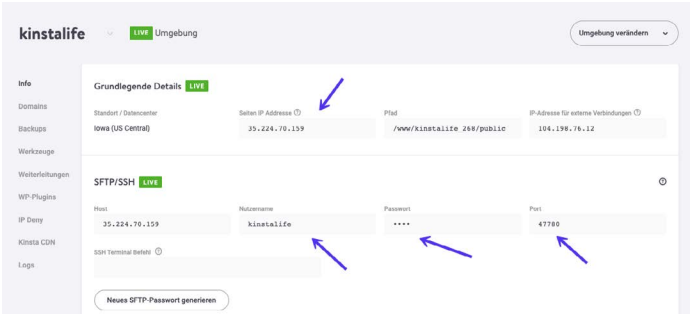


Eine zweite Empfehlung ist die Verwendung eines anderen Datenbanktabellen-Präfixes. Wenn Sie WordPress installieren, fragt es nach einem Tabellen-Präfix. Standardmäßig verwendet WordPress wp_. Wenn Sie dies auf etwas wie 39xw_ ändern, kann dies viel sicherer sein.

Wenn Sie ein Kinsta-Kunde sind und alle Webseiten Ihrer Kunden bei uns hosten, ist dies nicht erforderlich. Wir haben die Webseite und die Datenbank für Sie gesperrt!

Immer sichere Verbindungen verwenden

Wir können nicht genug betonen, wie wichtig es ist, sichere Verbindungen zu nutzen! Vergewissern Sie sich, dass Ihr WordPress Host Vorkehrungen trifft, wie z.B. das Anbieten von SFTP oder SSH. SFTP oder Secure File Transfer Protocol (auch bekannt als SSH-Dateiübertragungsprotokoll), ist ein Netzwerkprotokoll, das für Dateiübertragungen verwendet wird. Es ist eine sicherere Methode im Vergleich zum Standard-FTP.



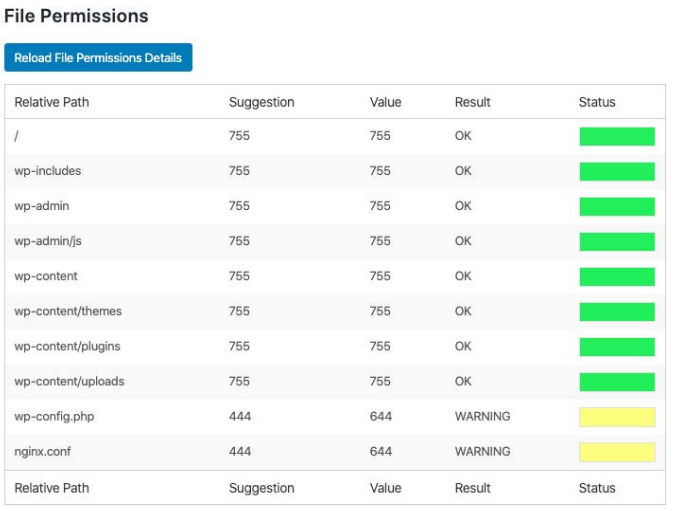
Schauen Sie sich diese Funktion mit der MyKinsta-Demo an.

Wir unterstützen bei Kinsta nur SFTP-Verbindungen, um sicherzustellen, dass Ihre Daten sicher und verschlüsselt bleiben. Die meisten WordPress-Hosts verwenden in der Regel auch Port 22 für SFTP. Wir gehen hier bei Kinsta noch einen Schritt weiter und jede Webseite hat einen zufälligen Port, den Sie in Ihrem MyKinsta-Dashboard finden können.

Datei- und Server-Berechtigungen prüfen

Dateiberechtigungen sowohl auf den Installationen Ihrer Kunden als auch auf den Webservern sind entscheidend für die Erhöhung der Sicherheit dieser Umgebungen. Wenn die Berechtigungen zu locker sind, könnte sich jemand leicht Zugang zu seiner Webseite verschaffen und Verwüstungen anrichten. Wenn Ihre Berechtigungen hingegen zu streng sind, könnte dies die Funktionalität der Seite beeinträchtigen. Daher ist es wichtig, die richtigen Berechtigungen für alle Beteiligten festzulegen.

Sie können ein kostenloses Plugin wie iThemes Security verwenden, um die Berechtigungen auf den WordPress-Seiten Ihrer Kunden zu scannen.



Hier sind einige typische Empfehlungen für Berechtigungen, wenn es um Datei- und Ordnerberechtigungen in WordPress geht:

- Alle Dateien sollten 644 oder 640 sein. Ausnahme: wp-config.php sollte 440 oder 400 sein, um zu verhindern, dass andere Benutzer auf dem Server sie lesen.
- Alle Verzeichnisse sollten 755 oder 750 sein.
- Kein Verzeichnis sollte jemals 777 erhalten, auch keine Upload-Verzeichnisse.

Eine ausführlichere Erklärung finden Sie im WordPress-Codex-Artikel über die Änderung von Dateiberechtigungen.

DDoS-Schutz

DDoS ist eine Art von DOS-Angriff, bei dem mehrere Systeme verwendet werden, um ein einzelnes System anzugreifen und einen Denial-of-Service-Angriff (DoS-Angriff) zu verursachen. DDoS-Angriffe sind nichts Neues - laut Britannica geht der erste dokumentierte Fall auf Anfang 2000 zurück. Im Gegensatz zu jemandem, der Ihre Webseite hackt, schädigen diese Arten von Angriffen normalerweise nicht Ihre Webseite, sondern bringen Ihre Webseite lediglich für ein paar Stunden oder Tage zum Erliegen.

Was können Sie tun, um sich zu schützen? Eine der besten Empfehlungen ist es, einen seriösen Sicherheitsdienst von Drittanbietern wie Cloudflare oder Sucuri zu nutzen.

Ihr fortschrittlicher DDoS-Schutz kann dazu verwendet werden, DDoS-Angriffe jeder Art und Größe abzuschwächen, einschließlich derjenigen, die auf die Protokolle UDP und ICMP sowie SYN/ACK, DNS-Verstärkung und Layer-7-Angriffe abzielen. Zu den weiteren Vorteilen gehört, dass Sie hinter einem Proxy stehen, der Ihre ursprüngliche IP-Adresse verbirgt, obwohl er nicht kugelsicher ist.

Übersehen Sie nicht den Provider, den Ihr Web-Host verwendet, denn auch das ist ziemlich wichtig.

Hardware-Firewalls, wie die Google Cloud Platform Firewall, die wir bei Kinsta verwenden, sind vorhanden und haben sehr enge softwarebasierte Einschränkungen, um die Webseiten Ihrer Kunden zu schützen, und verfügen auch über Software, um DDoS-Angriffe zu erkennen, wenn sie passieren.

Das bedeutet, dass Sie und Ihre Kunden von einem Sicherheitsmodell profitieren, das im Laufe von 15 Jahren aufgebaut wurde und derzeit Produkte und Dienstleistungen wie Google Mail, Suche usw. sichert. Google beschäftigt derzeit mehr als 500 Vollzeit-Sicherheitsexperten.

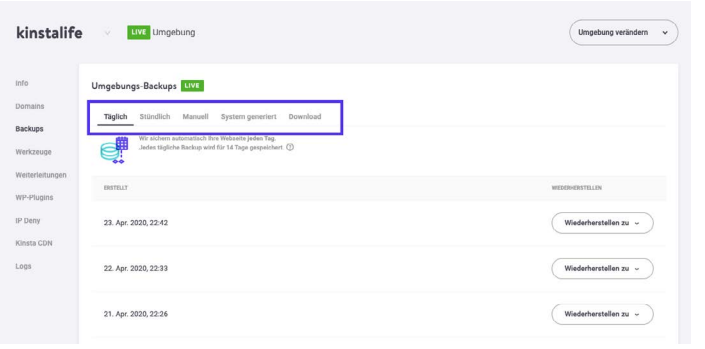
Neben der Google Cloud Platform verwenden wir auch Linux-Container (LXC und LXD), um sie zu orchestrieren, was es uns ermöglicht, nicht nur jedes Konto, sondern jede einzelne WordPress-Seite vollständig zu isolieren.

Trotzdem passiert etwas? Kinsta bietet kostenlose Hack-Reparatur und Malware-Entfernung. Wenn die Webseite einer Ihrer Kunden infiziert ist, wird unser Support-Team alles tun, was nötig ist, um die Webseite zu säubern.

Erfahren Sie mehr darüber, wie ernst wir die Sicherheit bei Kinsta nehmen! 

Immer Sicherungen machen

Ganz gleich, wie sicher Ihre Webseite ist, sie wird nie zu 100 % sicher sein. Deshalb machen Sie Backups für den Fall, dass das Schlimmste passiert. Backups sind das Einzige, von dem jeder weiß, dass er es braucht, das aber nicht immer gemacht wird. Die meisten der hier aufgeführten Empfehlungen sind Sicherheitsmaßnahmen, die Sie ergreifen können, um die Webseiten Ihrer Kunden und Ihr Unternehmen besser zu schützen.



Schauen Sie sich diese Funktion mit der MyKinsta-Demo an.

Die meisten verwalteten WordPress-Hosting-Provider bieten inzwischen Backups an. Kinsta bietet fünf verschiedene Arten von Backups an:

- Täglich: Kinsta erstellt alle 24 Stunden automatische Backups aller Webseiten Ihrer Kunden, damit Sie nachts ruhig schlafen können.

- Stündlich: Wenn Sie einen häufigeren Backup-Zeitplan benötigen, können Sie automatische Backups von 6 Stunden oder stündlich für jede Zielseite, die dies erfordert, aktivieren (dies kommt zu Ihrem Monatsplan hinzu).
- Manuell: Wenn automatische Backups nicht ausreichen, können Sie für jede von Ihnen verwaltete Webseite manuelle Backups erstellen und diese zusätzliche Kopie für 14 Tage oder länger, je nach Ihrem aktuellen Plan, zur Verfügung haben.
- Systemgeneriert: Bevor kritische Aufgaben wie die Verwendung des Suchen-Ersetzen-Tools in MyKinsta, die Live-Schaltung einer Staging-Umgebung und die Wiederherstellung eines Backups in Ihrer Live-Umgebung durchgeführt werden, löst Kinsta systemgenerierte Backups aus.
- Archiv zum Herunterladen: Wenn das alles nicht ausreicht, können Sie einmal pro Woche eine Zip-Datei jeder Kundenseite mit Webseite-Dateien und eine SQL-Datei mit dem Inhalt der Seiten-Datenbank herunterladen.

Die Backup-Optionen kommen aber nicht allein, da Kinsta es Ihnen ermöglicht, jede beliebige Webseite mit einem einzigen Klick wiederherzustellen. Das ist praktisch, nicht wahr?

Testen Sie kostenlos, wie einfach es ist, Backups mit MyKinsta zu erstellen!

Wenn Ihr Host keine Backups hat, gibt es einige populäre WordPress-Plugins, die Sie zur Automatisierung des Prozesses verwenden können.

WordPress Backup-Plugins

Mit den WordPress Backup-Plugins können Sie Ihre Backups per FTP abrufen oder in eine externe Speicherquelle wie Amazon S3, Google Cloud Storage, Google Drive oder Dropbox integrieren. Wir empfehlen dringend, eine inkrementelle Lösung zu verwenden, damit diese weniger Ressourcen verbraucht:

- Duplicator
- WP Time Capsule
- BackupBuddy
- UpdraftPlus
- BackUpWordPress
- BackWPup
- WP BackItUp

Kinsta erlaubt keine nicht-inkrementellen Backup-Plugins aufgrund von Leistungsproblemen: Wir handhaben all dies für Sie auf Serverebene, damit es die Webseiten Ihrer Kunden nicht verlangsamt.

Zusammenfassung

Sicherheit ist ein Schichtenspiel. Je mehr es Ihnen gelingt, neue Sicherheitsschichten übereinander zu stapeln, desto sicherer werden die Webseiten Ihrer Kunden. Alles beginnt damit, clevere Passwörter zu verwenden, den Core und die Plugins auf dem neuesten Stand zu halten und andere bewährte Sicherheitsmethoden zu befolgen, die wir hier behandelt haben.

Aber das ist nicht alles, was Sie tun sollten, um Ihre Chancen zu verringern, sich mit gehackten Kunden-Webseiten auseinanderzusetzen. Wenn Sie sich für einen verwalteten WordPress-Host wie Kinsta entscheiden, sind die meisten Sicherheitsmaßnahmen für Sie erledigt, so dass Sie eine solide, sichere und skalierbare Grundlage für die Sicherung der Zukunft der Webseiten Ihrer Kunden schaffen können und die Ihres Unternehmens.

Möchten Sie ausprobieren, wie einfach es ist, Kunden-Webseiten auf Kinsta zu verwalten? Schauen Sie sich demo.mykinsta.com an!


KINSTA