Whitepaper

Sucuri Website Security für Wordpress-Websites

Tipps für Dienstleister und WordPress-Seitenbetreiber

Powered by Sucuri

Domain Factory

Inhaltsverzeichnis

Management Summary

Sicherheit für WordPress – effizient und günstig

Mit einem Marktanteil von mehr als 35 Prozent ist WordPress das bei weitem populärste Content Management System (CMS) und für jeden Hacker ein lohnendes Ziel. Deshalb brauchen WordPress-Sites heute besonderen Schutz. Denn nicht nur die Zahl der Cyber-Attacken steigt ständig. Die Angriffe werden auch immer effizienter und ausgefeilter, und sie treffen bei WordPress und seinen vielen Tausend Plugins prinzipbedingt auf zahlreiche Schwachstellen.

Für Sie als Website-Betreiber und Dienstleister heißt das: Sie müssen sich entweder selbst genügend Security-Ressourcen und Kompetenzen aufbauen, um WordPress-Seiten effektiv zu schützen. Das ist problematisch, weil es viel Aufwand und ständige Aufmerksamkeit erfordert, aber selten genügend Budget dafür vorhanden ist.

Oder Sie greifen auf Sucuri Website Security zurück. Sucuri ist ein führender Anbieter von Website-Security-Lösungen und Services mit weltweiter Präsenz und als Kunde von DomainFactory können Sie kostengünstig und einfach auf die umfassenden cloudbasierten Website-Security-Services von Sucuri zurückgreifen.

Sucuri überwacht Ihre Websites auf Malware, SEO-Spam, DNS- oder SSL-Probleme, Beeinträchtigungen bei der Verfügbarkeit oder Blacklisting-Ereignisse. Ist eine Website kompromittiert, sorgen erfahrende Malware-Experten für eine schnelle und vollständige Bereinigung. Darüber hinaus schützt die CDN-basierte Sucuri Firewall Websites in Echtzeit vor Cyber-Bedrohungen wie Bad Bots, Hacking-Versuche, Zero-Day-Exploits, DDoS-Attacken oder Brute-Force-Angriffe. Sichere Backups, aktuelle Security-Informationen und globales Caching auf Sucuris Servern runden den Schutz ab.

Ihr Nutzen

Rundum-Schutz

Sucuri schützt Ihre WordPress-Site umfassend gegen Bedrohungen aus dem Netz.

Schnelle Hilfe bei Hacks & Infektionen

Auch im Schadensfall sind Sie mit Sucuri auf der sicheren Seite: dank jederzeit aktueller Backups und schneller, gründlicher Malware-Bereinigung durch Profis.

Maximale Verfügbarkeit

Verteilt auf Sucuri-Server weltweit und permanent überwacht, ist Ihre Website zuverlässig vor Ausfällen oder Überlastung geschützt.

Weniger Aufwand und Kosten

Mit Sucuri Website Security schützen Sie als Seitenbetreiber und Dienstleister Ihre WordPress-Sites deutlich kostengünstiger als mit vergleichbaren Angeboten.

WordPress braucht besonderen Schutz

WordPress ist Zielscheibe Nr. 1 für Hacker

Täglich werden weltweit mehr als 90.000 Websites gehackt (Quelle: Hosting Facts Internet Stats & Facts for 2019). Ein großer Teil dieser Websites läuft mit WordPress. Denn dieses ist das weltweit am häufigsten verwendete CMS – mehr als 36 Prozent aller Websites nutzen heute diese Plattform (März 2020; Tendenz steigend).

Aber nicht nur seine führende Marktstellung macht WordPress zu einem beliebten Ziel für Hacker- und Malware-Attacken. Hinzu kommen Tausende Schwachstellen im WordPress-Code. Sie verteilen sich auf WordPress-Core, Plugins und Themes; in der Praxis sind aber vor allem Plugins gefährdet.

Plugin Name	Installations
Easy WP SMTP	400,000
Wp File Manager	500,000
Fremius Library *(Multiple plugins are affected)*	200,000
Newspaper and other old tagDiv themes	100,000
WordPress GDPR Compliance	100,000
Social Warfare	70,000
WP Live Chat Support	60,000
Yuzo Related Post	60,000
WP-Piwik	60,000
My Sticky Menu	60,000

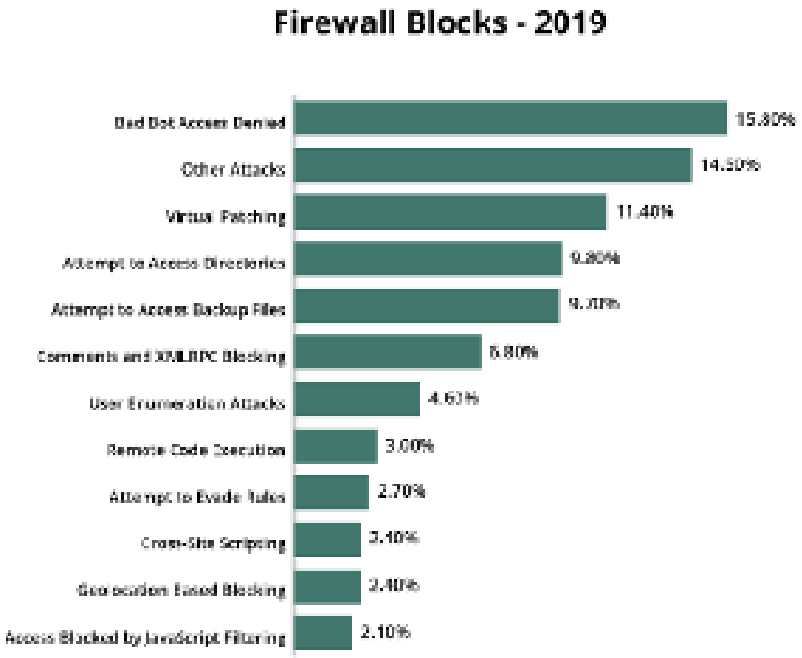
Top-10-Plugins (nach Installationen), die 2019 von der update_option()-Kampagne betroffen waren (Quelle: Sucuri)

Ein verbreiteter Angriffspunkt ist zum Beispiel die update_option()-Funktion von WordPress. Sie wird verwendet, um Einträge in der Options-Tabelle zu aktualisieren. Wenn Berechtigungen dafür nicht korrekt implementiert werden, können sich Angreifer Systemzugang mit Admin-Rechten verschaffen. 2019 gehörte diese Methode zu den häufigsten Infektionswegen – nach Angaben des Research-Teams von Sucuri waren davon in 2019 insgesamt 54 Plugins betroffen, mit Auswirkungen auf Millionen Websites weltweit (Quelle: Sucuri Website Threat Research Report 2019).

Automatisierte Angriffe nehmen zu

Hacker scannen mit Hilfe von Computerprogrammen (Bots) das Internet auf bekannte Sicherheitslücken ab und fahren zum Teil massive automatisierte Kampagnen, um diese zu monetarisieren. Durchschnittlich 60 Mal am Tag bekommt eine Website Besuch von Bad Bots (Quelle: Sitelock Security Report 2019).

Die Firewall von Sucuri blockierte in 2019 knapp 27 Millionen Bad-Bot-Angriffe, die damit unter den verzeichneten Angriffsarten Platz 1 einnahmen (Abbildung 2). Insgesamt blockierte die Sucuri Firewall fast 171 Millionen Angriffsversuche. Das entspricht einem Anstieg von 52 Prozent gegenüber 2018 (Quelle: Sucuri Website Threat Research Report 2019).



Die Sucuri Firewall blockierte 2019 fast 171 Millionen Angriffsversuche (Quelle: Sucuri).

Großes Schadenspotenzial

Findet ein Bad Bot oder eine Brute-Force-Attacke eine Schwachstelle, folgt meist automatisch ein gezielter Angriff. Das Schadenspotenzial ist riesig: Die direkten Auswirkungen reichen vom Datendiebstahl und der Übernahme der Website über Störungen und Umsatzeinbußen durch Downtimes bis hin zu hohen Lösegeldforderungen. Aber auch die indirekten Folgen können großen Schaden anrichten, etwa das sogenannte Blacklisting durch Suchmaschinen. Wenn Google & Co. Ihre Seiten für gefährlich halten und nicht mehr in ihren Suchergebnissen anzeigen oder Sicherheitswarnungen ausgeben („Diese Website kann Ihren Computer beschädigen"), kann das Ihr Image und das Kundenvertrauen erheblich beeinträchtigen. Pro Woche identifiziert der Dienst Google Safe Browsing ca. 30.000 Websites als potenziell schädlich. Ist eine Seite erst einmal in einer Blacklist eingetragen, kostet es viel Zeit und Aufwand, um sie wieder zu entfernen.

Fazit: WordPress-Installationen brauchen besonderen Schutz – und Sie als Betreiber oder Betreuer brauchen einen Plan B, wenn es trotzdem zu einer Kompromittierung kommen sollte. Denn 100-prozentige Sicherheit gibt es für Websites nicht.

Herausforderungen für Betreiber und Dienstleister

Hoher Sicherheitsbedarf bei Kunden

Der besondere Schutzbedarf von WordPress stellt Website-Betreiber und insbesondere auch Webdienstleister vor Herausforderungen. Ihre Kunden erwarten natürlich, dass Sie als ihr Webmaster oder Dienstleister auch für die Sicherheit der Website sorgen. So sind Dienstleister, die ihren Kunden auch Security-Leistungen anbieten können, gegenüber dem Wettbewerb klar im Vorteil.

Kunden sind aber leider häufig nicht bereit, solche Leistungen angemessen zu bezahlen. Denn viele Website-Betreiber haben keine Vorstellung davon, wie groß der Aufwand tatsächlich ist, um WordPress-Installationen abzusichern. Ist allerdings erst einmal ein Schaden eingetreten, macht der Kunde nicht selten doch wieder den Dienstleister oder Webmaster dafür verantwortlich.

Das Thema WordPress-Security ist komplex – hier einige Punkte, die dabei zu beachten sind.

WordPress aktuell halten ist wichtig, aber aufwendig

Werden Software-Schwachstellen entdeckt und offengelegt, liefern die Entwickler in der Regel schnell ein Update, das die Sicherheitslücke schließt. Das muss allerdings auch zeitnah eingespielt werden – ein Hauptgrund für erfolgreiche Malware-Infektionen sind veraltete Systeme. 49 Prozent aller WordPress-Sites, die das Sucuri-Team 2019 von Malware befreit hat, waren zum Zeitpunkt der Infektion veraltet (Quelle: Sucuri Website Threat Research Report 2019).

Zwar gibt es seit WordPress 3.7 eine automatische Update-Funktion. Diese aber richtet unter Umständen mehr Schaden an als Gutes: Bei jedem Update (ob von WordPress oder dem Plugin selbst) muss der Betreiber prüfen oder hoffen, dass noch alles reibungslos funktioniert – vor allem bei Installationen mit vielen Plugins ist das durchaus ein Problem. Viele Plugins erfahren kaum Qualitätssicherung und es gibt keine Garantien, dass eine neue Version mit der eingesetzten WordPress-Version und allen anderen Plugins reibungslos funktioniert. Nicht wenige Experten empfehlen daher, bestimmte Updates nur manuell und immer dann durchzuführen, wenn genügend Zeit fürs Testen zur Verfügung steht. Dann kann es aber auch passieren, dass das System mal eine Zeit lang mit einer kritischen Sicherheitslücke läuft. Das ist gefährlich, weil professionelle Hacker systematisch neu veröffentlichte Sicherheitspatches analysieren und oft innerhalb weniger Stunden einen angepassten Angriff starten können.
Eine weitere Möglichkeit sind automatisierte Tests, aber dafür fehlt vielen Website-Betreibern das Know-how.
Fazit: Die Aktualität und Funktionstüchtigkeit einer WordPress-Installation sicherzustellen kann sehr aufwendig sein, und Kompromisse gehen unweigerlich zu Lasten der Sicherheit.

Updates helfen nicht gegen Zero-Day-Exploits

Aber auch regelmäßige Updates bieten keine 100%ige Sicherheit – immerhin waren 51 Prozent der von Sucuri reparierten Websites schon auf dem neuesten Stand. Eine große Gefahr sind Angriffe auf Schwachstellen, die noch nicht geschlossen wurden, entweder weil sie den Entwicklern noch gar nicht bekannt sind (Zero-Day-Exploits) oder weil die Entwickler aus anderen Gründen noch keinen Patch liefern konnten. Allein im Februar 2020 wurden Zero-Day-Angriffe per Cross-Site-Scripting auf vier verbreitete WordPress-Plugins mit 100.000, 40.000 sowie 2 x 20.000 betroffenen Websites bekannt (Quelle: ZDNet).

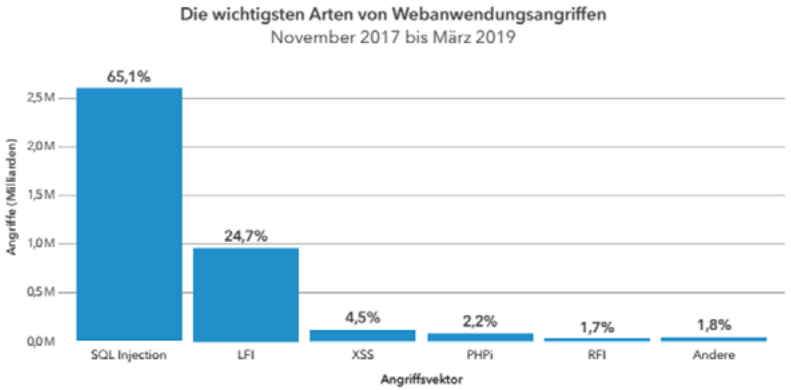
Updates helfen nicht gegen Brute-Force-Attacken

Eine andere Angriffsart, gegen die Updates allein nicht helfen, sind Brute-Force-Angriffe. Dabei probieren Hacker automatisiert viele Tausend oder Millionen Passwortkombinationen aus, um sich Zugang zum System zu verschaffen. Hier sind vor allem „schwache“ (also kurze, wenig komplexe, leicht zu erratende) Passwörter und Benutzernamen gefährdet, aber auch solche, die bei mehreren Konten Verwendung finden. Denn häufig nutzen die Kriminellen dafür gestohlene Datenbanken mit echten Zugangsdaten. Brute-Force-Attacken richten sich also gegen die „Schwachstelle Benutzer“ und machen sich Unwissenheit, Nachlässigkeit oder Bequemlichkeit Ihrer Anwender zu Nutze.

Bei WordPress richten sich Brute-Force-Attacken nicht immer nur gegen die Login-Seite (wp-login.php), sondern häufig auch direkt gegen die Datenbank selbst. Zwar verhindern Hoster normalerweise den externen Zugriff auf ihre Datenbanken, aber da meist Hunderte oder gar Tausende Websites auf den gleichen Datenbankserver zugreifen, müssen die Hacker nur eine davon übernehmen, um eine Brute-Force-Attacke auf die Datenbanken zu fahren. Hat eine der ausprobierten Kombinationen Erfolg, können sie etwa über die wp_options-Tabelle die URL der zugehörigen Website herausfinden.

Schutz manuell oder per Plugin

Weil Updates allein keine Sicherheit garantieren können, müssen bei WordPress-Installationen zusätzliche Sicherheitsmaßnahmen ergriffen werden. Wichtig ist dabei insbesondere der Schutz gegen die Angriffsmethoden SQL-Injektion (SQLI), Remote/Local File Inclusion (RFI/LFI) und Cross-Site Scripting (XSS). Injection-Angriffe liegen dabei unangefochten an der Spitze: Sie machen laut Akamai über 65 Prozent der Angriffe auf Webanwendungen aus (siehe Abbildung 3) und führen auch die viel zitierten OWASP Top Ten an.



SQL-Injection ist derzeit die häufigste Angriffsart.

Bei SQL-Injektionen werden böswillige Datenbankbefehle in SQL-Datenbanken eingeschleust, z. B. über manipulierte Formulareingaben. LFI bringt verwundbare Anwendungen dazu, unautorisiert auf lokal vorhandene Dateien zuzugreifen. XSS-Angriffe wiederum nutzen aus, dass Benutzereingaben (direkt vom Hacker oder etwa durch Klick des Opfers auf einen präparierten Link) ohne Prüfung an den Webbrowser des Opfers weitergesendet werden, der dann z. B. eingebetteten Code ausführt. Um solche Angriffe abzuwehren, muss die Unschädlichkeit von Nutzereingaben sichergestellt werden. So kann man Formulare etc. durch Captchas schützen und sollte zudem per Code stets den User-Input validieren und bereinigen sowie Datenausgaben bereinigen und maskieren.

Vielen Dienstleistern fehlt aber die Zeit und manchmal auch das Know-how, um diesen Aufwand zu bewältigen, zumal zur Absicherung noch sehr viel mehr gehört: regelmäßige Überprüfung auf Schwachstellen und Anzeichen für Sicherheitsprobleme (Indicators of Compromise), regelmäßige Backups, Schutz von Login-Formular und Datenbanken etc.

Deshalb werden viele Webmaster zu einem Security-Plugin für WordPress greifen, das einige dieser Aufgaben übernimmt. Aber Vorsicht: Hier kommt es auf die richtige Auswahl an, weil viele Plugins selbst Sicherheitsprobleme machen können – auch Security-Plugins.

Mit Sucuri Website Security sind Sie als WordPress-Sitebetreiber oder Dienstleister dagegen auf der sicheren Seite. Der Service kombiniert ein WordPress-Plugin mit Malware-Scans, Web Application Firewall, Whitelisting/Blacklisting-Funktionen sowie Backups und schützt dank CDN auch vor DDoS-Angriffen.

Kundenseiten infiziert – was tun?

Cyberangriffe werden nicht nur immer häufiger, sondern auch komplexer. Das erschwert Analyse und Bereinigung, wenn eine Website tatsächlich kompromittiert wird. Andererseits erwarten Website-Betreiber dann eine schnelle Reaktion von ihrem Dienstleister oder Webmaster, weil mit jedem Tag der Schaden wächst.

Umfragen zufolge hatte fast die Hälfte der Webdienstleister schon einmal mit einer gehackten Kundenseite zu tun (Quelle: Sucuri Web Professional Security Survey 2019). Die manuelle Bereinigung einer mit Malware infizierten Website erfordert viel Zeitaufwand und auch viel Know-how. Denn moderne Malware versteckt sich meist an vielen Stellen einer Website gleichzeitig und oft auch noch auf anderen

Websites auf dem gleichen Server, installiert Backdoors und bringt auch Selbstheilungsmechanismen mit, um bei unvollständiger Bereinigung die Site erneut zu infizieren. So fanden sich auf fast 30.000 infizierten Websites (von über 60.000, die Sucuris Malware-Experten in 2019 bereinigt haben) eine oder mehrere Backdoors (Quelle: Sucuri Website Threat Research Report 2019).

Das grundsätzliche Vorgehen bei der Bereinigung einer gehackten Website sieht so aus (mehr Informationen hier):

Informationen sammeln:

1. Malware-Scan (mit Sucuri SiteCheck, dem WordPress-Plugin von Sucuri oder einem anderen Tool, am besten sowohl remote als auch serverseitig.
2. Integritätsprüfung von WordPress-Core-Dateien in wp-admin, wp-include und Stammverzeichnis, am besten im Vergleich zu den Dateien eines sauberen Backups
3. Kürzlich geänderte Dateien überprüfen, sie könnten Teil des Hacks sein
4. Nutzung der Diagnosefunktionen z. B. von Webmaster-Tools oder von Google Safe Browsing, falls die Website auf die Google-Blacklist geraten ist

Site bereinigen:

1. Backup erstellen
2. Verdächtige Core-Files durch originale Dateien aus dem offiziellen Repository ersetzen
3. Verdächtige Custom-Files durch Backup-Kopien ersetzen
4. Falls das nicht möglich ist, mit einem Text-Editor verdächtigen Code entfernen
5. Testen, ob die Site ordnungsgemäß funktioniert.

Dieses Vorgehen setzt voraus, dass Sie über spezifisches Wissen zur Bedrohung verfügen. Wenn Sie beim Malware-Scan fündig werden, erhalten Sie bereits wertvolle Hinweise, womit Sie es zu tun haben. Hatten Sie allerdings persönlichen Besuch von einem Hacker, müssen Sie sich auch auf Überraschungen gefasst machen. Wie schon deutlich wurde, ist dann auch ein sauberes und halbwegs aktuelles Backup nützlich. Wurde allerdings ein Angriff erst nach einiger Zeit festgestellt, können auch Backups schon infiziert sein. Es kann dann durchaus passieren, dass eine komplette Wiederherstellung des Zustands unmittelbar vor der Infektion nicht mehr möglich ist.

Sicherheit und Mehrwert mit Sucuri

Sicherheit kostet Aufwand, erst recht die professionelle Reaktion auf eine gehackte Seite. Auch wenn Kunden oft nicht bereit sind, für Security-Services zu zahlen, erwarten sie doch entsprechende Leistungen. Angesichts wachsender Cyber-Bedrohungen ist das für Webdienstleister ein Teufelskreis.

Mit Sucuri Website Security lösen Sie Security-Probleme professionell und kostengünstig – von der Prävention bis zur Bereinigung. Sucuri bietet nicht nur einen Rundum-Schutz für WordPress-Websites, sondern informiert die Verantwortlichen auch über mögliche Probleme und aktuelle Sicherheitslücken.

Für WordPress-Betreiber ist Sucuri auch deshalb besonders geeignet, weil das Team auf einen großen Erfahrungsschatz mit diesem CMS zurückgreifen kann. Knapp 95 Prozent der aktuellen Sucuri-Kunden setzen WordPress ein (Quelle: Sucuri Website Threat Research Report 2019).

Zudem können Webdienstleister damit ihren Kunden einen Mehrwert bieten, den kaum ein Mitbewerber im Portfolio hat. Denn die wenigsten Webdienstleister bieten einzelne Website-Security-Services an. Nicht einmal 10 Prozent der Dienstleister können Websites aktiv vor Malware-Angriffen schützen. Immerhin knapp 12 Prozent bieten Malware-Scans und 14 Prozent Backups. Dem steht gegenüber, dass zwei Drittel der Websitebetreiber sich Security-Leistungen wünschen (Quelle: Sucuri Web Professional Security Survey 2019; siehe Abbildung 4). WordPress-Dienstleister erhalten mit Sucuri maßgeschneiderten Schutz und verschaffen sich zusätzlich einen Vorsprung im Wettbewerb.

Nur wenige Webdienstleister können ihren Kunden Security-Leistungen anbieten (Quelle: Sucuri)

Szenarien

Praxisbeispiel 1: Malwareinfektion und Blacklisting rückgängig machen

Ein Mitarbeiter des Kunden hat eine Website gefunden, auf der Premium-Themes kostenlos angeboten werden. Er lädt sich ein besonders schönes Theme herunter, um es auszuprobieren. Das Theme ist mit der Malware WP-VCD infiziert. Obwohl der Kunde das Theme wieder löscht, nistet sich der Schadcode in der CMS-Installation ein.

Hintergrund

Die Hacker-Gruppe WP-VCD hostet manipulierte Raubkopien von Premium-Themes oder Plugins auf eigenen SEO-optimierten Websites. Einmal installiert, schleust die WP-VCD-Malware eigene Dateien ein, ändert Core-Files von WordPress und schreibt Backdoor-Code in die functions.php aller gefundenen Themes, der mit einem Command- & Control-Server kommuniziert. Einige Versionen richten auch ein neues Admin-Konto ein. Anschließend sucht sie auf dem Server nach weiteren WordPress-Installationen, um auch diese zu infizieren. Die Malware besitzt Selbstheilungsfunktionen, die bei unvollständiger Bereinigung eine erneute Infektion versuchen.

Die Folgen ohne Sucuri

Die Malware injiziert SEO-Spam, spielt dubiose Werbung aus, leitet Besucher per 301-Redirect um und nervt sie mit Popups. Besucher springen ab, der Traffic bricht ein. Google erfährt von der Infektion und setzt die Website auf seine Blacklist. Nun kommt der Webtraffic fast vollständig zum Erliegen. Nachfragen häufen sich, Vertrauensverlust und Imageschäden drohen.

Der Kunde macht Druck und fordert die Behebung des Problems. Der Webdienstleister muss nun herausfinden, womit er es zu tun hat, sich die erforderlichen Informationen beschaffen und die Kunden-Website mühsam per Hand bereinigen. Da er erst Wochen nach der Infektion benachrichtigt wurde, ist dennoch bereits ein erheblicher Schaden eingetreten.

Die Lösung mit Sucuri Website Security

Noch bevor der Kunde etwas davon bemerkt, entdeckt Sucuri die Infektion. Der Webdienstleister wird automatisch benachrichtigt und erteilt sofort den Auftrag zur Bereinigung. Den brauchen die Profis von Sucuris SIRT, damit sie die nötigen Veränderungen an der Kundenwebsite durchführen dürfen.

Sucuris Security-Experten analysieren die Kundenwebsite und erkennen schnell das Problem, denn WP-VCD ist seit Jahren für einen Großteil der WordPress-Infektionen verantwortlich. 2019 fand das Sucuri-Team auf mehr als 5.000 infizierten Kunden-Websites die WordPress-Malware WP-VCD (Quelle: Sucuri Website Threat Research Report). Die Spezialisten bereinigen sämtliche infizierten Dateien und prüfen auch alle anderen WordPress-Installationen des Accounts. Sie können dabei auf ein aktuelles Backup zurückgreifen – Sucuris Backup-Dienst speichert in einstellbaren Abständen automatisch Dateien und Datenbanken auf externen Servern im Suruci-Netzwerk. Zum Schluss überprüfen sie alle wichtigen Blacklists und sorgen dafür, dass überall das Blacklisting rückgängig gemacht wird.

Das Ergebnis:

Die Website ist bereits wenige Stunden nach der Infektion vollständig wiederhergestellt. Dem Webdienstleister sind dadurch keine zusätzlichen Kosten entstanden – und er wird von Sucuri proaktiv über weitere erkannte Probleme und neue Sicherheitslücken informiert, damit sich der Vorfall möglichst nicht wiederholt.

Praxisbeispiel 2: WordPress-Kundenseiten proaktiv absichern

Nachdem die WordPress-Website eines Partnerunternehmens Opfer eines Hacks geworden war, sollen die eigenen Seiten abgesichert werden.

Die Folgen ohne Sucuri

Das Unternehmen überprüft und verbessert die internen Richtlinien für Berechtigungen und starke Passwörter und organisiert Security-Schulungen für die Mitarbeiter, an denen aber nicht alle Teammitglieder teilnehmen. In WordPress wird die automatische Backup-Funktion aktiviert und alle eingesetzten Plugins werden auf bekannte Schwachstellen überprüft. Nach eingehender Prüfung wird aber auch klar, dass inhouse nicht genügend Ressourcen und Know-how verfügbar sind, um manuell eine permanente Komplettabsicherung zu gewährleisten. Für die Absicherung von Datenbank und Benutzereingaben wird ein Security-Plugin installiert.

Trotzdem wird die Website infiziert, weil eines der eingesetzten Plugins eine Schwachstelle aufweist, für die der Entwickler noch keinen Patch bereitgestellt hat. Die Verantwortlichen erfahren davon aber erst nach einiger Zeit, weil ihnen Kunden mitteilen, dass sie beim Klick auf Links der Seite zum Beispiel auf Pornoseiten umgeleitet werden. Ein spezialisierter Dienstleister wird mit der Bereinigung der Seiten beauftragt und stellt dafür einen hohen dreistelligen oder vierstelligen Betrag in Rechnung. Dafür müssen dem Dienstleister sämtliche Website-Daten ausgehändigt werden – einschließlich sensibler Kundendaten aus dem Service-Bereich. Gemäß den Vorgaben der DSGVO müssen sämtliche betroffenen Kunden davon informiert werden.

Die Lösung mit Sucuri Website Security

Der Webmaster bestellt bei seinem Hoster DomainFactory das Security-Paket Sucuri Deluxe und das zugehörige Wordpress-Plugin. Er installiert das Plugin über sein WordPress-Plugin, aktiviert das Plugin mit einem von DomainFactory mitgelieferten Code und kann sofort mit der Konfiguration beginnen.

Mit wenigen Mausklicks über das Sucuri Dashboard aktiviert der Webmaster die regelmäßige serverseitige und Remote-Überprüfung auf Malware. Werden Anzeichen für eine Kompromittierung gefunden, wird der Webmaster automatisch informiert und kann bei Sucuri die kostenlose Bereinigung beauftragen.

Außerdem aktiviert der Webmaster die Sucuri Firewall, die den kompletten Netzwerkverkehr überwacht und so einen Echtzeit-Schutz vor verschiedensten Bedrohungen bietet, einschließlich Malware-, DDoS- und Brute-Force-Angriffen. Dafür nutzt sie ein weltweit verteiltes Content-Delivery-Network (CDN), in dem sie Kopien der geschützten Website ablegt, und eigene DNS-Dienste, die auch für bessere Performance und Verfügbarkeit der Website sorgen. Per Virtual Patching kann die Sucuri Firewall zudem Anwendungen gegen Exploits ungeschützter Schwachstellen absichern.

Weil Service und Preis-Leistungs-Verhältnis stimmen, steigt das Unternehmen nach einigen Monaten auf das Paket Sucuri Ultimate um. Denn dieses bietet noch einmal mehr Sicherheit durch automatische Backups, mit denen im Ernstfall der Zustand eines beliebigen Tages der letzten drei Monate wiederhergestellt werden kann.

Mit dem Sucuri Vertrauenssiegel kann das Unternehmen seinen Websitebesuchern zudem zeigen, dass Sicherheit ihm am Herzen liegt.

So schützt Sucuri

Sucuri Website Security sorgt für den professionellen Schutz Ihrer Websites vor Hackern, Malware, Datenverlusten, DDoS- und Brute-Force-Angriffen oder Zero-Day-Exploits.

Website-Überwachung

Das Intrusion Detection System von Sucuri überwacht Ihre Webseiten regelmäßig auf Anzeichen für Kompromittierungen (Indicators of Compromise). Dazu gehören zum Beispiel Schadcode, SEO-Spam, Einschränkungen der Verfügbarkeit, Unregelmäßigkeiten bei SSL-Zertifikaten und DNS-Einstellungen oder auch Blacklistings.

Sucuri greift bei der Überwachung auch auf eine eigene Bad-Domain-Blacklist zurück. Damit entdeckte Sucuri SiteCheck 2019 auf über 137.000 Websites mehr als 450.000 Ressourcen von Bad Domains, darunter auf mehr als 125.000 Websites auch bösartige Ressourcen, die andere Blacklist-Betreiber übersehen hatten. Auf 40 Prozent dieser Seiten fanden sich Skripte von nur 10 Bad Domains, die alle mit einer einzigen massiven WordPress-Infektion assoziiert waren (Quelle: Sucuri Website Threat Research Report 2019).

Das Monitoring kann sowohl remote (getarnt als Website-Besucher) als auch serverseitig erfolgen. Bei Problemen wird umgehend der Website-Betreiber oder Dienstleister informiert.

Malware-Beseitigung

Erhalten Anwender durch Sucuri oder aus anderen Quellen Kenntnis von einem Malware-Problem, können sie mit wenigen Mausklicks und ohne Mehrkosten eine professionelle Bereinigung durch Sucuris Incidence

Response Team beauftragen. Ohne ausdrückliche Erlaubnis führt Sucuri keine Änderungen an Kunden-Websites durch.

Nach Beauftragung wird Sucuri zuverlässig innerhalb der zugesicherten Reaktionszeit aktiv, im Tarif „Express“ nach spätestens 30 Minuten. Gestützt auf Sucuris umfassende Threat Intelligence, analysieren die erfahrenen Security-Spezialisten von Sucuri sorgfältig die komplette Website und ihre Server-Umgebung, entfernen nachhaltig Malware, Backdoors, SEO-Spam, Redirects, Verunstaltungen (Defacements) und alle anderen Spuren der Kompromittierung und stellen die volle Funktionsfähigkeit der Website wieder her. Zudem sorgen sie dafür, dass eventuelle Blacklist-Eintragungen rückgängig gemacht werden.

Echtzeit-Schutz vor Angriffen

Die Sucuri-Firewall kombiniert eine cloudbasierte Website Application Firewall (WAF) mit einem Intrusion Prevention System (IPS). Als Reverse Proxy inspiziert sie alle eingehenden HTTP/HTTPS-Requests an eine Website und entfernt böswillige Anfragen, bevor sie den Webserver des Kunden erreichen.

Auf Applikationsebene schützt Sucuri vor Malware- und Hacker-Angriffen per SQLI, XSS, RFI/LFI etc. sowie vor DDoS- und Brute-Force-Attacken. Weitere Funktionen beinhalten u. a. die Analyse und Überwachung von Netzwerkverkehr und Logs, Zugriffskontrolle für kritische Seiten per IP-Whitelisting, Geoblocking sowie Virtual Patching & Hardening.

Optimierte Verfügbarkeit und Performance durch CDN

Die Sucuri Firewall basiert auf einem global verteilten, leistungsfähigen Content Delivery Network. Statischer Webcontent wird auf CDN-Knoten in den USA, Europa, Asien, Australien und Brasilien zwischengespeichert.

Dadurch wird nicht nur die Verfügbarkeit Sucuri-geschützter Webseiten verbessert, sondern auch ihre Performance kann dadurch verbessert werden: durch weniger Datenbankabfragen, kürzere Laufwege zwischen Client und auslieferndem Server.

Backup-Sicherung und Wiederherstellung

Sucuri Website Security beinhaltet einen Backup-Service, der auf Wunsch alle Website-Dateien und Datenbanken für drei Monate automatisch speichert – täglich, wöchentlich oder monatlich. Das Backup erfolgt auf Sucuris hochsichere Infrastruktur außerhalb der Hosting-Umgebung und damit unerreichbar für Hacker und Malware.

So kann bei Bedarf, etwa nach einem Malware-Befall oder einem Serverproblem, mit wenigen Mausklicks eine saubere, funktionsfähige Version aus den letzten 90 Tagen komplett wiederhergestellt werden.

Sucuri Website Security: Das richtige Paket für Ihre WordPress-Anforderungen

DomainFactory bietet die Services von Sucuri Website Security in vier unterschiedlichen Paketen an. Damit erhalten Sie als Website-Betreiber oder Dienstleister für Ihre WordPress-Sites genau die Sicherheitsfeatures, die Sie benötigen.

Der günstige Basisschutz: Sucuri Essential

Das Paket Sucuri Essential bietet den grundlegenden Schutz, den heute jede Website haben sollte. Es beinhaltet regelmäßige Malware-Scans, Überwachung auf Blacklisting und im Bedarfsfall die Beseitigung gefundener Probleme durch das Sucuri-Team (Reaktionszeit 12 Stunden nach Auftrag).

Rundum sicher: Sucuri Deluxe

Das Paket Sucuri Deluxe ist vor allem für Websites ausgelegt, bei denen es auf eine hohe Sicherheit und Performance ankommt, zum Beispiel für Webshops oder geschäftskritische Webanwendungen mit sensiblen Daten. Es umfasst alle Leistungen des Basisschutzes (Sucuri Essential) sowie die Blockade von Hacking- und Angriffsversuchen durch die CDN-basierte Sucuri Firewall.

Sicherheit und Verfügbarkeit: Sucuri Ultimate

Das Komplettpaket Sucuri Ultimate ist das Angebot für Websitebetreiber mit höchsten Anforderungen an Sicherheit und Verfügbarkeit. Das Paket ergänzt die Leistungen von Sucuri Deluxe durch Backup und Restore und eine kürzere Reaktionszeit (6 Stunden).

Schnelle Hilfe: Sucuri Express

Es kommt auf jede Minute an? Dann ist Sucuri Express die richtige Wahl. Dieses Paket beinhaltet ebenfalls alle Leistungen von Sucuri Deluxe und darüber hinaus die sofortige Hilfe bei Problemen mit einer garantierten Reaktionszeit von maximal 30 Minuten.

Alle Sucuri-Pakete auf einen Blick

Sucuri Website Security **Essential**	Sucuri Website Security **Deluxe**	Sucuri Website Security **Ultimate**	Sucuri Website Security **Express**
Das günstige Einstiegspaket für kleine Webprojekte wie Ihre eigene Webseite	Durchsucht repariert und schützt Ihre Webseite	Schutzfunktionen mit besonders kurzer Reaktionszeit	Schnelle Hilfe in nur 30 Minuten
0,99 €/ 1. Monat danach 4,99 € mtl.* **Bestellen**	**4,99** €/ 1. Monat danach 19,99 € mtl.* **Bestellen**	**9,99** €/ 1. Monat danach 29,99 € mtl.* **Bestellen**	**299,99** €/im Jahr **Bestellen**
Reaktionszeit 12 Stunden	**Reaktionszeit** 12 Stunden	**Reaktionszeit** 6 Stunden	**Reaktionszeit** 30 Minuten
Malware-Scan einer einzelnen Website	**Malware-Scan** einer einzelnen Website	**Malware-Scan** einer einzelnenWebsite	**Malware-Scan** einer einzelnenWebsite
Malware-Beseitigung Unbegrenzt	**Malware-Beseitigung** Unbegrenzt	**Malware-Beseitigung** Unbegrenzt	**Malware-Beseitigung** Unbegrenzt
Google-Blacklisting Überwachung und Beseitigung	**Google-Blacklisting** Überwachung und Beseitigung	**Google-Blacklisting** Überwachung und Beseitigung	**Google-Blacklisting** Überwachung und Beseitigung
	Web Application Firewall ✓	**Web Application Firewall** ✓	**Web Application Firewall** ✓
	CDN ✓	**CDN** ✓	**CDN** ✓
		Backup & Restore ✓	

Mehr Informationen

Weiterführende Informationen finden Sie auf unserer Website www.df.eu/de/sucuri-website-malware-scanner.
Bei konkreten Fragen können Sie sich auch gern direkt an uns wenden.
Unser Produktberatungsteam erreichen Sie telefonisch unter
+49 89 998 288 031 (Mo-Fr 9–17 Uhr).


Domain Factory