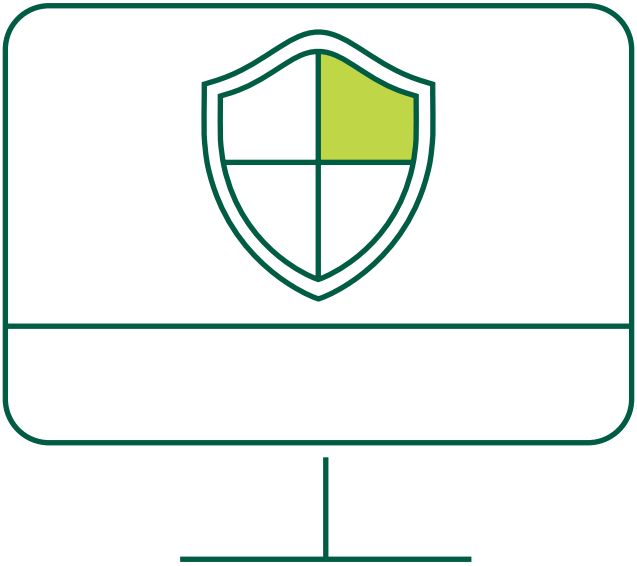
DomainFactory präsentiert

Website Security

Powered by Sucuri

DomainFactory

Inhaltsverzeichnis



Sucuri Website Security

Würden Sie Ihre Fenster offenlassen, während Sie im Urlaub sind? Würden Sie Ihren Laptop unbeaufsichtigt herumliegen lassen? Wahrscheinlich nicht. Ihre ungeschützte Website kann auf ähnliche Weise ein leichtes Ziel für Diebe oder Eindringlinge sein.

Das Internet kann ein gefährlicher Ort sein und jeder ist ein potenzielles Angriffsziel. Täglich werden über 90.000 Websites gehackt.

Es spielt keine Rolle, ob Sie ein äußerst beliebtes Unternehmen betreiben oder nur 1.000 Besucher pro Monat verzeichnen. Malware und Hacker machen keinen Unterschied. Tatsächlich sind die meisten Malware-Angriffe automatisiert, was bedeutet, dass Sie genauso Ziel sind wie jeder andere.

Kleine Unternehmen sind besonders beliebt

Die Einstellung: “Mir wird das nicht passieren” kann fatal sein. Wenn Sie der Meinung sind, dass Hacker nur größere Unternehmen ins Visier nehmen und keinen Grund haben, Ihre Website anzugreifen, täuschen Sie sich.

Vorbei sind die Zeiten, in denen die meisten Hacker es nur auf Großunternehmen abgesehen haben. Tatsächlich sind von 65% der Cyber-Angriffe kleine und mittlere Unternehmen betroffen. Warum ist das so? Viele von ihnen sind sich der Gefahr nicht bewusst und nehmen es mit der Sicherheit ihrer Website nicht so genau.

Ein Hacker kann leichter auf kleinere Websites zugreifen als auf große Unternehmen wie PayPal oder Facebook, bei denen einige der besten Sicherheitsingenieure rund um die Uhr daran arbeiten, solche Hacks zu

verhindern. Hier einige weitere Zahlen, die die tatsächliche Bedrohung durch Cyber-Angriffe verdeutlichen:

- 54% der Unternehmen weltweit geben an, im letzten Jahr mindestens einmal angegriffen worden zu sein
- Nur 38% der Unternehmen sind auf Cyber-Angriffe vorbereitet
- Der durchschnittliche Ransomware-Angriff kostet ein Unternehmen 5 Millionen US-Dollar

Mit 230.000 neuen Malware-Attacken, die jeden Tag stattfinden, sieht es nicht so aus, als würden Hacker-Angriffe zurückgehen. Im Gegenteil, 60% der kleinen Unternehmen bestätigen, dass die Angriffe immer schwerwiegender und raffinierter werden.

Keine Website ist gegen Cyber-Angriffe immun

Die meisten Websites werden nicht direkt von einer Person gehackt. Hacker erstellen Scripte, die rund um die Uhr Domains bzw. Websites nach Sicherheitslücken durchsuchen. Sobald sie fündig werden, sind die Scripte normalerweise so programmiert, dass sie eine oder mehrere der folgenden Aufgaben ausführen:

- Sie infizieren die Computer oder Endgeräte Ihrer Besucher mit Malware oder bösartiger Software
- Sie stehlen die Informationen von Personen, die Ihre Website besuchen oder darauf vertrauliche Informationen eingeben
- Sie leiten Ihre Besucher auf bösartige oder andere Websites um, die für sie Affiliate-Einnahmen generieren
- Sie senden Spam-E-Mails, bis Ihre Website von Google auf die Blacklist gesetzt wird

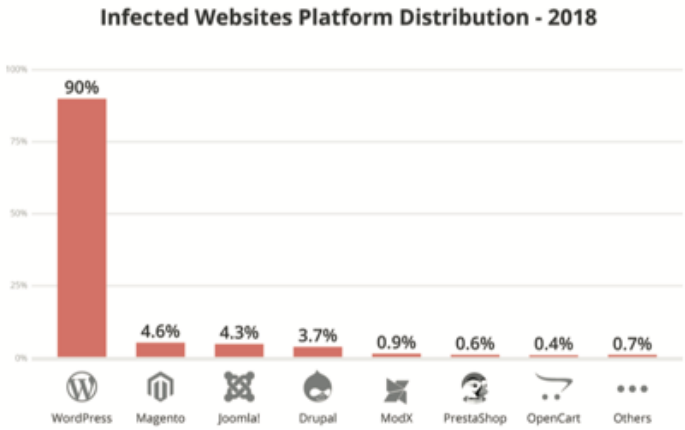
- Sie platzieren auf Ihrer Seite eine eigene Nachricht, um Ihre Website unbrauchbar zu machen und Besucher zu vertreiben

Sobald ein Hacker einen Zugang findet, kann er die Kontrolle über Ihre Website übernehmen, alle Informationen aus Ihrer Datenbank stehlen und sie zu seinem Vorteil nutzen. Worst-Case-Szenario? Es kann so weit gehen, dass Sie Lösegeld an Hacker zahlen müssen, um wieder auf Ihre Website zugreifen zu können.

WordPress zieht Hacker magisch an

Laut dem Website-Hack-Trendbericht 2018 von Sucuri wurden 90% der über 25.000 analysierten infizierten Websites auf der WordPress-Plattform erstellt - im Vergleich zu 83% im Jahr 2017.

Dem Bericht zufolge liegt das Problem nicht bei der Plattformsicherheit, sondern unter anderem bei “unsachgemäßer Bereitstellung, Problemen mit der Sicherheitskonfiguration und mangelndem Sicherheitswissen oder mangelnden Ressourcen”.



Dies sind die Hauptgründe, die WordPress zu einem Magneten für Hacker machen. Es liegt nicht allein an der Popularität, sondern auch an dem Mangel an Wissen, Ressourcen und Verständnis der Benutzer, wenn es darum geht, ihre Website abzusichern und vor Cyberangriffen zu schützen.

Da mittlerweile über ein Drittel aller Websites im Internet mit WordPress erstellt wurden, besteht für einen großen Teil des Internets eine erhöhte Gefahr eines Cyberangriffs.

Tatsächlich ergab Sucuris Bericht, dass es sich bei dem primären Angriffsvektor auf mit WordPress erstellten Websites um Plugins mit bekannten und unbekannten Schwachstellen handelte.

Den meisten Websitebesitzern ist nicht bewusst, wie anfällig ihre Website ist – bis es zu spät ist

Der Bericht von Sucuri zeigt: Eines der größten Probleme ist das mangelnde Verständnis, wie wichtig die fortlaufende Wartung und die regelmäßige Überprüfung auf Sicherheitslücken für die Sicherheit sind.

Wussten Sie, dass ein Hacker durchschnittlich 146 Tage in einem Netzwerk verbringt, bevor er entdeckt wird? Normalerweise ist der Prozess langsam und unauffällig, und Angreifer bleiben oft monatelang oder länger unbemerkt. Bis Sie also feststellen, dass Sie angegriffen wurden, ist es zu spät und der Schaden ist bereits entstanden.

Erschreckender ist, dass Hacker auch nach einer Bereinigung heimlich in ein Netzwerk zurückkehren können. Sie richten oft Hintertüren ein, damit sie die vollständige Kontrolle über eine gesamte Website erlangen und jederzeit zurückkehren können.

Cyberangriffe können Sie Ihr Geschäft kosten

Sobald ein Hacker Zugriff hat, kann er mehr als nur Ihre Website zerstören. Innerhalb weniger Minuten kann ein Cyberangriff Ihren Ruf und das Vertrauen Ihrer Kunden, an dem Sie jahrelang gearbeitet haben, ruinieren.

Es kann so weit gehen, dass Ihre Website von Suchmaschinen wie Google auf die Blacklist gesetzt wird, wodurch Ihr Unternehmen für die digitale Welt unsichtbar wird.
Diese Zahlen sollten Sie diesbezüglich kennen:

- Cyberangriffe kosten kleine Unternehmen zwischen 84.000 und 148.000 US-Dollar
- 43% der Nutzer verlassen Websites, wenn Sicherheitswarnungen angezeigt werden
- Websites verlieren etwa 95% ihres Traffics, wenn sie von Google auf die Blacklist gesetzt werden

Nehmen Sie die Sicherheit Ihrer Website ernst ergreifen Sie die erforderlichen Schutzmaßnahmen. Hier erfahren Sie, warum Sucuri Website Security eine unverzichtbare Lösung ist, um das Risiko eines Cyberangriffs zu verringern und Ihr Online-Geschäft sicher und erfolgreich zu machen.

Was ist Sucuri Website Security?

Ihre Website ist wertvoll für Ihr Unternehmen. Schützen Sie sie proaktiv vor drohenden Sicherheitslücken! Der Schutz Ihrer Online-Präsenz mag auf den ersten Blick vielleicht zeitaufwändig und teuer scheinen – aber das muss nicht sein. Nicht, wenn Sie die richtige Lösung kennen.

Einfach – leistungsfähig – zuverlässig

Sucuri Website Security ist unser neues cloudbasiertes Website Security-System, mit dem Ihre Website vor Online-Bedrohungen geschützt wird. Es ist eine besonders einfache und wirkungsvolle Möglichkeit, Ihre Website vor Hackern, Malware, DDoS und weiteren Angriffsformen sowie vor Blacklisting zu schützen.

Das funktioniert folgendermaßen: Um den Sicherheitsstatus zu ermitteln, wird Ihre Online-Präsenz kontinuierlich überwacht. So kann schädlicher Code erkannt und neutralisiert werden, bevor er überhaupt auf Ihre Website gelangt.

Sucuri, eine angesehene Marke im Bereich SaaS-Sicherheitssoftware, kümmert sich für Sie um die Sicherheit Ihrer Website und Sie haben diese Sorge weniger.

So profitieren Sie von unserer Website Security-Lösung:

Unbegrenztes Scannen, Erkennen und Entfernen von Malware

Hacker verwenden automatisierte Skripte, um Websites zu finden und sofort zu infizieren. Je schneller Ihre Website nach einem Angriff repariert wird, umso geringer sind die negativen Auswirkungen auf Ihren Traffic, Ihr Ansehen und Ihre Suchmaschinenoptimierung.

Aus diesem Grund scannen wir Ihre Website täglich bis zur Serverebene und stellen sicher, dass sie frei von Malware, schädlichem JavaScript, schädlichen iframes, verdächtigen Umleitungen, eingefügten Spam-Links und vielem mehr ist.

Wenn Ihre Website-Dateien, Datenbanken, DNS-Einträge und SSL-Zertifikate verdächtige Inhalte enthalten, werden Sie umgehend benachrichtigt. Je früher Sie unser Expertenteam beauftragen, desto eher arbeiten wir daran, das Problem zu beheben und Ihre Website wieder sicher zu machen.

Wir überwachen auch die Verfügbarkeit Ihrer Website, um sicherzustellen, dass sie immer erreichbar ist und ordnungsgemäß funktioniert. Sollte Ihre Website ungewollt offline sein, können Sie sofort Maßnahmen ergreifen und sie schnell wieder online stellen, damit Ihre Besucher nicht davon betroffen sind.

Überwachung und Entfernung aus der Google-Blacklist

Sie haben viel dafür getan, um die Sichtbarkeit Ihrer Website auf den Suchergebnisseiten von Google zu verbessern. Wenn Ihre Website angegriffen wird, verlieren Sie nicht nur Ihre Rankings, sondern werden auch von Google auf die Blacklist gesetzt und somit für Ihre potenziellen Besucher unsichtbar.

Website Security hilft Ihnen, Ihr Ranking und Ihren Ruf intakt zu halten. Es verhindert auch, dass Ihre Besucher abschreckende Warnungen wie diese sehen:

Wie? Indem Website Security ständig überprüft, ob Ihre Website nicht von bekannten Suchmaschinen wie Google oder anderen Institutionen wie zum Beispiel Norton oder Opera auf die Blacklist gesetzt wurde.

Falls Ihre Website mit Malware infiziert ist und von Google auf die Blacklist gesetzt wird, werden wir Ihre Website bereinigen.

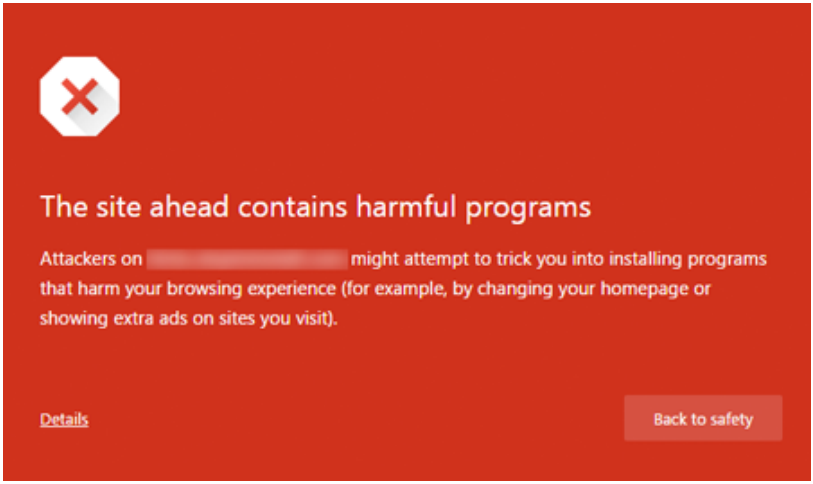
Verteidigen Sie Ihre Website schon im Vorfeld mit einer Web Application Firewall (WAF)*

Täglich tauchen neue Malware-Infektionen und -Bots auf. Glücklicherweise ist unsere cloud-basierte Firewall-Lösung leistungsstark genug, um Ihre Website vor DDoS-, Injection-, Brute-Force-, XSS- und Zero-Day-Angriffen zu schützen.

Dazu wird der gesamte Traffic auf Ihrer Website in Echtzeit geprüft, schädlicher Traffic herausgefiltert und nur erwünschter Traffic zugelassen. Dies hilft nicht nur, Angriffe zu verhindern, bevor sie überhaupt passieren – es macht Ihre Website auch schneller, da die Serverauslastung erheblich sinkt.

Verbesserte Ladezeit und Leistung Ihrer Website*

Ein positives Kundenerlebnis zu bieten, bedeutet auch, Ihre Besucher nicht länger als drei Sekunden auf das Laden Ihrer Website warten zu lassen. Die Leistungssteigerung durch ein Content Delivery Network (CDN) verleiht Ihrer Website nicht nur eine zusätzliche Sicherheitsebene, sie macht sie auch performanter und schneller.



Superschnelle Reaktionszeit

Sollte ein Angreifer all diese Sicherheitsbarrieren überwinden und irgendwie Zugriff auf Ihre Website erlangen, müssen Sie uns nur darüber informieren. In spätestens 12 Stunden reagiert unser Expertenteam und arbeitet so lange an Ihrer Website, bis die Bedrohung beseitigt ist. Wenn Sie Hilfe benötigen, sind wir rund um die Uhr für Sie da.

** Nicht im Tarif Essential enthalten*

Wie schützt Sucuri?

Sucuri Website Security schützt Ihre Website in vier Schritten:

1. Reagieren

Sie können sich nicht vor etwas schützen, das sie gar nicht kennen. Einige Hacks sind schwer zu entdecken, da sie nicht offensichtlich sind. Und selbst, wenn sie es wären, haben Sie als Kleinunternehmer nicht die Zeit, Ihre Website jeden Tag extern und intern auf mögliche Sicherheitslücken zu überprüfen.

Sucuri Website Security scannt Ihre Website jeden Tag sorgfältig auf Online-Bedrohungen, Malware und Sicherheitslücken, auch auf dem Server. Es überwacht alles von der Datei-Integrität über Probleme mit dem Front-End bis hin zu nicht autorisierten Änderungen an DNS-Einträgen und SSL-Zertifikaten.

Wenn Malware versucht, Ihr System zu infizieren, können Sie sicher sein, dass Sucuri Website Security sie entdeckt, sodass Sie sie sofort stoppen können.

Das Tool hilft Ihnen auch, die Rankings Ihrer Website zu schützen und sie in den Suchmaschinen sichtbar zu halten. Es überwacht die Sicherheitswarnungen der Google-Blacklist und stellt sicher, dass Ihre Website ordnungsgemäß funktioniert und nicht auf die “Schwarze-Liste“ gesetzt wurde.

2. Warnen

Wenn Malware gefunden wird, werden Sie darüber informiert. Sucuri Website Security kennzeichnet verdächtige Unregelmäßigkeiten auf Ihrer Website und sendet Ihnen umgehend eine Warnmeldung, damit Sie eine Malware-Bereinigungsanforderung an unser Expertenteam senden können.

Von da an übernehmen unsere Sicherheitsexperten die Reparatur Ihrer Website, bis diese zu 100% bereinigt ist. Betrachten Sie uns als Ihre persönliche schnelle Eingreiftruppe.

Nach einer Reaktionszeit von maximal 12 Stunden arbeitet unser Team rund um die Uhr daran, die Malware zu entfernen und Ihre Website zu reparieren, bis Ihre Website wieder sicher ist, egal wie lange es dauert.

3. Sichern

Hacker sind schlau. Mit viel Zeit und den neuesten Techniken finden sie Sicherheitslücken in den unzähligen Codezeilen, aus denen Ihre Website besteht, und verschaffen sich Zugriff auf alle Ihre Dateien.

Glücklicherweise macht unsere Web Application Firewall (WAF) dies unmöglich. WAF verwendet eine Whitelist-Methode, die diese Fehler für Angreifer unbrauchbar macht. Sie wirkt wie ein Schutzschild um Ihre Website und verhindert Angriffe von vornherein.

Wenn Sie diesen zusätzlichen Schutz wünschen, richten Sie unsere Web Application Firewall ein (verfügbar mit Sucuri Deluxe, Ultimate und Express).

Unsere wirkungsvolle WAF bietet eine zusätzliche Sicherheitsebene, um eine erneute Attacke zu verhindern und Ihre Website in Zukunft vor Malware und Angriffen zu schützen. Dazu gehören:

- DDoS-Attacken (einschließlich Layer 7 HTTP-Flood-Angriffe)
- Brute-Force-Angriffe, bei denen Hacker jede mögliche Kombination aus Benutzername und Passwort in Ihrem Anmeldefeld ausprobieren, um die richtige Kombination zu finden und Zugriff auf Ihre Website zu erhalten.
- Zero-Day-Patches als Sofortmaßnahme. Dies ist ein Angriff, der erfolgt, sobald eine neue Sicherheitslücke entdeckt wird, noch bevor ein Patch verfügbar ist. Unsere WAF wird Ihre Site virtuell patchen und stärken, um unbefugten Zugriff zu verhindern und sie bis zum Sicherheitsupdate schützen
- Website-Attacken und Hacks
- Malware-Infektionen

4. Optimieren

Nicht nur Google liebt schnell ladende Websites, sondern auch Ihre Besucher und Kunden. Unser integriertes Content Delivery Network (CDN) beschleunigt Ihre Website um über 70%, unabhängig davon, wo Sie sich befinden. Das CDN speichert Ihren Content auf mehreren Servern weltweit, sodass er Ihren Besuchern schneller zur Verfügung gestellt werden kann.

Was ist, wenn Sie bereits gehackt wurden?

Sucuri Website Security hilft Ihnen nicht nur, Malware und Hacker zu erkennen und fernzuhalten, sie kann auch gehackte Websites reparieren.*

Kaufen Sie ein Sucuri Website Security Paket und beauftragen Sie uns umgehend – in spätestens 12 Stunden tritt unser Expertenteam in Aktion.

Sie wünschen schnellere Hilfe? Kein Problem. Wählen Sie das Paket Express, und unser Expertenteam reagiert innerhalb von 30 Minuten nach Erhalt Ihrer Anfrage.

Zunächst scannen wir Ihre Website, um Daten zu sammeln und zu analysieren. Wir geben diese Informationen dann an unser Expertenteam weiter, das Ihren Server und Ihre Datenbank durchsucht, um mögliche Anzeichen einer Gefährdung zu finden. Schließlich werden unsere Experten jede Malware entfernen, bis Ihre Website zu 100% bereinigt ist.

Sie kümmern sich auch darum, dass Google Ihre Website von der Blacklist entfernt und Ihr Unternehmen so schnell wie möglich wieder auf den Ergebnisseiten der Suchmaschinen erscheinen kann.

** Nicht im Tarif Essential enthalten*

Wie werden Schäden behoben?

Wenn Ihre Website mit Malware infiziert wird, sind wir für Sie da. Unser Expertenteam wird Ihnen bei jedem Schritt zur Seite stehen, jeglichen schädlichen Code entfernen und sicherstellen, dass Ihre Website schnell wieder funktioniert.

Sie werden benachrichtigt, sobald ein Problem gemeldet wird

Sucuri Website Security enthält die Tools, die Sie benötigen, um über den Zustand Ihrer Website informiert zu bleiben. Wenn unsere Deep-Scan-Engine verdächtige Aktivitäten oder Sicherheitslücken auf Ihrer Website entdeckt, werden Sie sofort darüber informiert.

Standardmäßig erhalten Sie eine Benachrichtigung über die E-Mail-Adresse, mit der Sie sich registriert haben. Sie können auch andere E-Mail-Adressen hinzufügen und Benachrichtigungen über SMS, Slack und mehr einrichten.

Ebenfalls werden Sie benachrichtigt, wenn Ihre Website aus irgendeinem Grund nicht mehr aufrufbar ist. Dies ist Teil unserer Uptime-Überwachung. Sein sie sich somit sicher, dass Sie schnell Maßnahmen ergreifen können, wenn Ihre Besucher nicht auf Ihre Website zugreifen können, damit Sie keine potenziellen Kunden und Umsätze verlieren.

Wir bieten außerdem wöchentliche oder monatliche E-Mail-Berichte über die Sicherheit Ihrer Website an. Dazu gehört eine Zusammenfassung der durch unseren Überwachungsprozess gefundenen Daten, die Sie wahlweise als reine Text- oder HTML-Datei erhalten.

Unser 24/7-verfügbares Website Security Team behebt Ihre Probleme

Wenn Sie eine Warnung erhalten, dass Ihre Website infiziert wurde, können wir umso schneller in Aktion treten, Schäden beheben und die Sicherheit Ihrer Website wiederherstellen, je schneller Sie unser Team benachrichtigen.

Sie können uns zu jeder Zeit mit der Entfernung von Malware beauftragen. Unser Expertenteam steht Ihnen rund um die Uhr zur Verfügung und reagiert innerhalb von 12 Stunden. Sie werden Ihre Website schnell bereinigen, sodass auf Ihrer Website oder Ihrem Server keine Spur von Malware mehr zu finden sein wird.

So identifizieren wir das Problem

Zunächst sammeln wir Informationen, um den Schaden zu bewerten. Wir führen einen vollständigen Sicherheitsscan auf Ihrer Website und Ihrem Server durch, sammeln die Daten und analysieren sie. Auf diese Weise können wir Ihre Umgebung schnell verstehen und bekannte Probleme und verdächtigen Code identifizieren. Wir sammeln auch Informationen über Ihre Website, Ihre Serverumgebung und etwaige Blacklisting-Warnungen. Wir überprüfen:

- Das CMS und die Erweiterungen, die auf Ihrer Site verwendet werden
- Bekannte Probleme und Anomalien im Quellcode
- Aktuelle Versionen Ihrer Website-Software
- Integritätsprobleme im Vergleich zu einer bekannt guten Ausgangsbasis
- Malware-Infektionen und Anzeichen einer Gefährdung

Sobald wir alle erforderlichen Daten gesammelt haben, geben wir sie an einen der hochqualifizierten Sicherheitsexperten weiter, die für Ihren Fall zuständig sind.

Wir nehmen Ihre Website und Ihren Server genau unter die Lupe

Hacker sind schlau. Sie wissen, dass Sie versuchen werden, Ihre Website zu bereinigen, sodass sie regelmäßig Hintertüren einbauen, um sich bei Bedarf erneut heimlich Zugriff auf Ihre Website zu verschaffen.

Das wollen wir auf jeden Fall verhindern. Aus diesem Grund werden unsere Experten alles auf Ihrer Website und Ihrem Server genau unter die Lupe nehmen. Sie werden ihr ganzes Know-How einsetzen, um alle Hintertüren, anfällige Software- und Serverkonfigurationsprobleme zu finden und sicherstellen, dass alle Anzeichen für eine Gefährdung erkannt und behoben werden.

Das Ergebnis: eine 100% saubere und sichere Website

Sobald wir alle benötigten Daten haben, entfernen wir sämtlichen schädlichen Code aus Ihren Website-Dateien und der Datenbank. Ihr Sicherheitsexperte überprüft dann die Integrität Ihrer Website, um sicherzustellen, dass alles sauber und funktionsfähig ist.

Als Nächstes werden wir uns bemühen, die Reputation Ihrer Marke in den Suchmaschinenergebnissen zu verbessern, damit Sie Ihre Sichtbarkeit und Ihren Traffic wieder in den Griff bekommen. Wir entfernen alle Blacklist-Warnungen zu Ihrer Website und beantragen bei Google, Ihre Website von der Blacklist zu nehmen. Dies erspart Ihnen die Zeit und den Aufwand, sich selbst darum kümmern zu müssen.

Anschließend wollen wir Sie unterstützen, dass Sie dieses Procedere so schnell nicht wieder durchlaufen müssen. Deshalb wird Ihnen unser Expertenteam nach dem Hack einige wichtige Schritte und Tipps senden und Sie beraten, wie Sie auch in Zukunft für die Sicherheit Ihrer Website sorgen.

Was macht Sucuri Website Security sonst noch?

Wir leben in einer schnelllebigen Welt. Jeder hat viel zu tun und braucht alles so schnell wie möglich. Website-Besucher werden schnell ungeduldig, wenn etwas zu lange dauert.

Kennen Sie die Ladezeiten Ihrer Website? Statistiken zufolge warten 47% der Nutzer nicht einmal zwei Sekunden auf das Laden einer Website. Wenn das Laden Ihrer Seiten mehr Zeit in Anspruch nimmt, haben Sie möglicherweise bereits Ihren potenziellen Kunden verloren.

Geschwindigkeit ist nicht nur für Ihre Besucher wichtig, sondern auch für Google. Der Suchmaschinenriese weiß, dass Nutzer einen schnellen Zugriff auf Informationen wünschen, weshalb Websites, die schnell geladen werden, belohnt werden (und Websites mit schleppendem Ladevorgang heruntergestuft werden).

Deshalb sind unsere Deluxe-, Ultimate- und Express-Pakete mit einem Content Delivery Network (CDN)-Leistungsbeschleuniger ausgestattet, mit dem Sie die Leistung und Geschwindigkeit Ihrer Website steigern können.

Wie funktioniert CDN?

Ein CDN beschleunigt Ihre Website, indem der physische Abstand zwischen Ihren Besuchern und dem Server Ihrer Website verringert wird. Dafür wird eine Version ihres Inhalts automatisch an mehreren Orten gespeichert.

Wenn also jemand in London auf Ihre in in Deutschland gehostete Website zugreift, erfolgt dies über einen Point of Presence (PoP) in Großbritannien. Auf diese Weise erhalten Ihre Besucher eine Version Ihrer

Website, die ihnen am nächsten ist, und Ihre Website lädt somit auf der ganzen Welt schneller. Wir speichern Ihre Website-Ressourcen an sechs hochverfügbaren Points of Presence (PoP) auf der ganzen Welt. Diese PoPs sind so konfiguriert, dass sie maximale Verfügbarkeit und Erreichbarkeit gewährleisten.

Außerdem verwenden wir die hochwertigsten Netzwerkports mit vier verfügbaren Caching-Ebenen, um eine deutlich verbesserte Reaktionszeit Ihrer Website zu gewährleisten.

So profitieren Sie davon

Die Verwendung unseres CDN-Leistungsbeschleunigers bietet viele Vorteile. Hier sind die wichtigsten:

1. Sie bieten eine optimale Benutzererfahrung

Der erste Eindruck im Web ist von entscheidender Bedeutung. Bereits beim ersten Besuch auf Ihrer Website fällen Besucher ein Urteil über Ihr Unternehmen.

Lädt Ihre Website langsam, halten ihre Besucher sie für instabil, nicht vertrauenswürdig und nicht sicher. So entsteht ein schlechter Eindruck, der langfristig zu einem negativen Image Ihrer Marke führen kann. Eine schnelle Website hingegen wirkt professionell, zuverlässig und vertrauenswürdig. Wenn Ihre Website also schnell geladen wird, haben Sie sofort einen positiven ersten Eindruck hinterlassen.

Unser CDN kann Ihnen dabei helfen, indem es den Zugriff auf Ihre Website beschleunigt, sodass auch Ihre ungeduldigsten Besucher schnell auf die benötigten Informationen zugreifen können.

2. Sie steigern Ihre Sichtbarkeit in den Suchmaschinenergebnissen

Sie wissen, dass Geschwindigkeit ein Rankingfaktor für Google und andere Suchmaschinen ist. Das ergibt ja auch Sinn. Eine Website mit langsamer Ladezeit und einer hohen Bounce-, Exit- und Abbruchrate weist Google darauf hin, dass ihre Besucher unzufrieden sind und dass diese Seite von Google nicht hoch gerankt und damit bevorzugt empfohlen werden sollte.

Google geht davon aus, dass nur eine schnelle Nutzererfahrung eine gute Nutzererfahrung ist. Aus diesem Grund werden schnell ladende Websites mit einem höheren Ranking belohnt.

Unser CDN-Leistungsbeschleuniger kümmert sich auch um dieses Problem, sodass Sie sicher sein können, dass Ihre potenziellen Kunden Ihr Unternehmen schnell ganz oben in den Suchergebnissen finden können.

3. Sie verschlüsseln den Datentransfer zwischen dem Browser des Benutzers und der Firewall

Die Deluxe- und Ultimate-Pakete der Sucuri Website Security bieten die Verschlüsselung vom Browser zu unserem CDN.

Wir empfehlen Ihnen, zusätzlich zur Sucuri Website Security ein separates SSL-Zertifikat zu nutzen, um Ihre Website, Ihre Kunden und alle Ihre Daten zu schützen.

Sie wollen Sucuri Website Security nutzen?

Nichts leichter als das. Sie können das Paket Ihrer Wahl auf unserer Seite sofort bestellen. Sobald Ihre Bestellung bestätigt und Sucuri Website Security zu Ihrem Control Panel hinzugefügt wurde, können Sie alle Vorteile nutzen.

- Gehen Sie auf https://www.df.eu/
- Melden Sie sich mit Ihrem Benutzernamen und Ihrem Passwort in Ihrem Kundenmenü an
- Im Menü unter Produkte und Software finden Sie Sucuri
- Klicken Sie auf Konfiguration

Hier können Sie Ihre Website hinzufügen und verwalten, Scans ausführen und Berichte überprüfen. Zu Beginn folgen Sie am besten diesen Schritten:

1. Schritt: Wählen Sie die Website aus, auf die Sie Sucuri Website Security anwenden möchten

Zunächst müssen Sie Ihre Website zum Dashboard hinzufügen.

2. Schritt: Geben Sie den Domainnamen ein

Geben Sie als Nächstes die URL ein, die Sie schützen möchten.

3. Schritt: Folgen Sie diesen Anweisungen

Sie werden jetzt zu Ihrem Website Security-Dashboard weitergeleitet. Um die Einrichtung abzuschließen, müssen Sie den Verfügbarkeitsscanner und E-Mail-Berichte aktivieren. Wenn Sie ein Paket mit WAF gekauft haben, sind einige weitere Schritte auszuführen, um es zu aktivieren.

Sie werden feststellen, dass Sie die Einstellungen auch abhängig von Ihrem gewählten Paket und Ihren Bedürfnissen ändern können. Sie können beispielsweise die Scan-Häufigkeit, Warnoptionen und mehr festlegen.

4. Schritt: Führen Sie einen Scan durch und prüfen Sie das Ergebnis

Website Security beginnt automatisch mit dem Scannen Ihrer Website. Je nach Größe Ihrer Website kann dies bis zu einer Stunde dauern. Nach dem Scannen werden Ihnen folgende Informationen über Ihre Website angezeigt:

- Warnungen vor Malware
- Wurde Ihre Website auf die Blacklist gesetzt – und wenn ja: von wem?
- Funktioniert Ihre Website ordnungsgemäß, sind Ausfallzeiten aufgetreten?
- Sind Änderungen an Ihren DNS-Einträgen und Ihrem SSL-Zertifikat vorgenommen worden?

Zwischen diesen Optionen können Sie wählen

Sucuri Website Security ist eine leistungsstarke Lösung für jede Website, unabhängig von der Größe oder Branche. Wir haben vier unterschiedliche Pakete zusammengestellt, sodass jeder Website-Besitzer genau die gewünschte Art von Sicherheit auswählen kann und nur für das bezahlt, was er wirklich benötigt.

Essential

Das Paket Essential ist ideal, wenn Sie grundlegenden Schutz wünschen. Es umfasst unbegrenztes und tägliches Scannen Ihrer Website, Erkennen und Entfernen von Malware, um Ihre Website frei von Schadsoftware zu halten. Sollte Ihre Website jemals mit Malware infiziert sein, erhalten Sie eine Warnmeldung, damit Sie sofort Maßnahmen ergreifen können.

Außerdem beobachten wir die Google-Blacklist für Sie. Das bedeutet, dass wir Ihre Website im Auge behalten und sicherstellen, dass keine Blacklist-Warnungen vorliegen. Wenn unsere Scans feststellen, dass Ihre Website auf die Blacklist gesetzt wurde, werden wir uns darum kümmern, sie so schnell wie möglich wieder daraus zu entfernen.

Wenn Sie bei uns die Entfernung von Malware oder die Entfernung aus einer Blacklist anfordern, reagieren unsere Experten, die rund um die Uhr arbeiten, in spätestens 12 Stunden.

Deluxe

Zusätzlich zum Scannen, Erkennen und Entfernen von Schadprogrammen und Blacklistings sowie der maximalen Reaktionszeit von 12 Stunden des Essential-Pakets enthält das Deluxe-Paket zwei weitere Funktionen für zusätzliche Sicherheit und Performance Ihrer Website.

Zum einen **schützt unsere Web Application Firewall (WAF) Sie vor Malware und Angriffen.** Sie installiert eine weitere Sicherheitsebene, indem sie verdächtigen Datenverkehr blockiert und nur erwünschten Traffic zulässt. Damit ist Ihre Website vor erneuten Infektionen sowie vor künftigen Schadprogrammen und Angriffen wie DDoS, Injektion, Brute Force, Cross-Site und Zero Day geschützt.

Zum anderen kann unser **CDN-Leistungsbeschleuniger** die Geschwindigkeit und Leistung Ihrer Website erheblich verbessern. Da sowohl Ihre Besucher als auch Google schnelle Ladezeiten schätzen, können Sie einen hervorragenden ersten (und zweiten und dritten und ...) Eindruck auf potenzielle Kunden machen, die Ihr Unternehmen in den Suchmaschinenergebnissen schneller finden.

Ultimate

Mit dem Security-Paket Ultimate nutzen Sie alle Funktionen des Deluxe-Pakets. Dies bedeutet Malware-Scanning, -Erkennung und -Entfernung, Google-Blacklist-Überwachung und -Beseitigung, Malware- und Angriffsprävention mit unserer Web Application Firewall sowie Leistungs- und Geschwindigkeitsoptimierung dank CDN. Ihre Website ist damit nicht nur vollständig vor Schadprogrammen und gefährlichen Angriffen geschützt, sondern wird auch schneller und performanter.

Dank ihrer **Backup- und Restore-Funktion** bietet das Ultimate-Paket zusätzliche Sicherheit. Im schlimmsten Fall können Sie sicher sein, dass Sie immer Zugriff auf ein vollständiges gesichertes Backup Ihrer Website haben. So können Sie mit nur einem Klick Ihre Website wiederherstellen.

Dieses Paket bietet Ihnen auch eine schnellere Reaktionszeit. Sollte es Probleme geben, wird unser Expertenteam innerhalb von sechs Stunden nach Ihrer Kontaktaufnahme in Aktion treten.

Express

Wenn Ihre Website gehackt wurde und Sie eine sofortige Schadensbehebung benötigen, ist das Express-Paket genau das richtige für Sie. Spätestens 30 Minuten nach Ihrer Anfrage scannt unser Expertenteam Ihre Website und arbeitet so lange an ihr, bis sie zu 100% sicher ist.

Außerdem beantragen wir in Ihrem Namen, dass Google Ihre Website aus der Blacklist entfernt und neu indiziert, damit sie wieder in den Suchergebnisseiten der Suchmaschine erscheint.

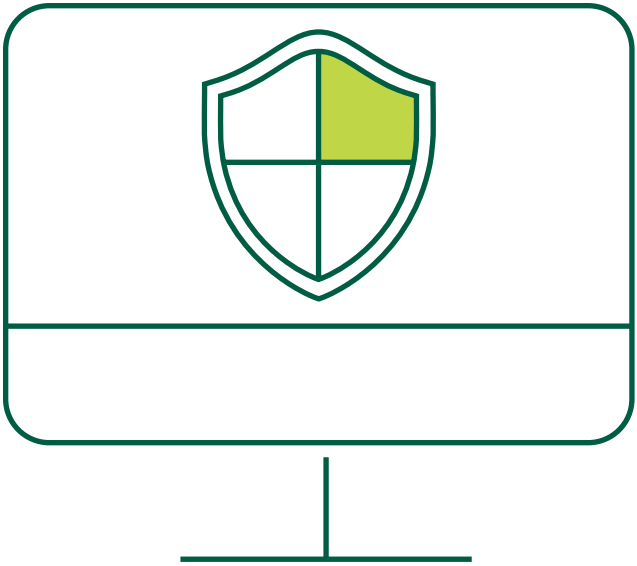
Mit unserer Web Application Firewall profitieren Sie außerdem von unbegrenzten Malware-Scans, ihrer Erkennung und Entfernung. Die WAF schützt präventiv vor Malware und Angriffen, überwacht das Blacklisting von Google und entfernt Ihre Website gegebenenfalls daraus. Darüber hinaus sorgt CDN für eine Leistungs- und Geschwindigkeitsoptimierung.

Schutz für mehrere Websites

Derzeit ist Sucuri Website Security mit einzelnen Käuferkonten verbunden, sodass das Control Panel nicht an andere Benutzer weitergegeben werden kann. Wir arbeiten aber bereits an der Entwicklung einer Reseller-Version.

Wenn Sie sich gerne um die Sicherheit der Websites Ihrer Kunden kümmern möchten, bieten wir Ihnen Vorzugspreise an beim Kauf von drei oder mehr Paketen in einem Bestellvorgang. Sprechen Sie bei Bedarf bitte unseren Support an.

Sucuri Website Security **Essential**	Sucuri Website Security **Deluxe**	Sucuri Website Security **Ultimate**
Das günstige Einstiegspaket für kleine Webprojekte wie Ihre eigene Webseite	Durchsucht, repariert und schützt Ihr Webseite	Schutzfunktionen mit besonders kurzer Reaktionszeit
0,99 €/im 1. Monat danach 4,99 € mtl.* **Bestellen**	**4,99** €/im 1. Monat danach 19,99 € mtl.* **Bestellen**	**9,99** €/im 1. Monat danach 29,99 € mtl.* **Bestellen**
Reaktionszeit 12 Stunden	**Reaktionszeit** 12 Stunden	**Reaktionszeit** 12 Stunden
Malware-Scan Unbegrenzte Seitenzahl	**Malware-Scan** Unbegrenzte Seitenzahl	**Malware-Scan** Unbegrenzte Seitenzahl
Malware-Beseitigung Unbegrenzt	**Malware-Beseitigung** Unbegrenzt	**Malware-Beseitigung** Unbegrenzt
Google-Blacklisting Überwachung und Beseitigung	**Google-Blacklisting** Überwachung und Beseitigung	**Google-Blacklisting** Überwachung und Beseitigung
	Web Application Firewall ✓	**Web Application Firewall** ✓
	CDN ✓	**CDN** ✓
		Backup & Restore ✓



Referenzen

https://sucuri.net/reports/2018-hacked-website-report
https://sucuri.net/reports/web-professional-security-survey-2019
https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html
https://wordpress.org/news/2019/03/one-third-of-the-web/
https://www.securitymagazine.com/articles/87288-the-costs-and-risks-of-a-security-breach-for-small-businesses


Domain Factory