Host Europe

Website Security powered by Sucuri

So optimieren Sie Sicherheit, Verfügbarkeit
und Performance für Ihre Websites

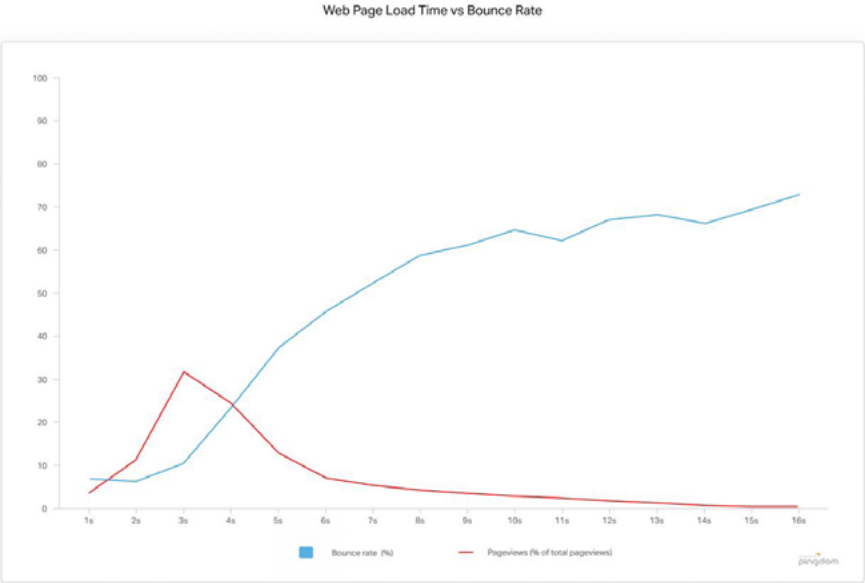
E-Book Teil 2

Inhaltsverzeichnis

Sucuri in der Praxis – Tipps für Profis

Performance und Sicherheit optimieren per CDN

Web-Nutzer sind ungeduldig. Die Absprungrate bei Webseiten ist umgekehrt proportional zu ihren Ladezeiten: Während bei einer Ladezeit von bis zu zwei Sekunden durchschnittlich sieben Prozent der Besucher eine Seite wieder verlassen, sind es bei 4 Sekunden Ladezeit bereits 24 Prozent (5 s: 38 %; 6 s: 46 %; 8 s: 59 %, ...).[1]



[1] Pingdom: Does Page Load Time Really Affect Bounce Rate?

Weil die Sucuri Firewall auf einem **Content Distribution Network (CDN)** basiert, können wir mit Hilfe verschiedener Caching-Optionen die Leistung Sucuri-geschützter Websites optimieren – im Durchschnitt um 70 Prozent!

Wie Sucuri Ihre Website-Performance optimiert

Das Sucuri-CDN nutzt ein globales Anycast-Netzwerk mit zehn Points of Presence in den USA, Europa und Asien und zwei CDN-Edges in Australien und Brasilien.

Die Zwischenspeicherung der Inhalte Ihrer Website über alle Knoten im Netzwerk hinweg (Caching) gewährleistet weltweit eine optimale Leistung.

Bei Seitenaufrufen werden die gewünschten Inhalte nicht von Ihrem Server, sondern vom jeweils nächstgelegenen CDN-Knoten ausgeliefert. Das beschleunigt die Reaktionszeit Ihrer Seiten.

Basierend auf den Sucuri-eigenen **DNS**-Diensten können wir in unserem CDN eine effektive geografische Lastverteilung (Loadbalancing) realisieren. Das weltweite Caching schützt Ihre Seite zudem vor Netzwerkausfällen.

Die Standardkonfiguration für Websites haben wir bereits auf hohe Leistung optimiert und auch das neue, latenzoptimierte **HTTP**-Protokoll HTTP/2 aktiviert. HTTP/2 wird von allen wichtigen Browsern und von über 40 Prozent aller Websites weltweit unterstützt.[2]

[2] W³Techs: **Usage Statistics of HTTP/2 for Websites (September 2019)**

Mit unseren flexiblen Caching-Optionen bestimmen Sie, wie häufig der Cache geleert wird. Die Standard-Einstellung ist **„Enabled"**. Bei **„Minimal Caching"** werden die Inhalte nur wenige Minuten gecacht. Mit der Einstellung **„Site Caching"** können Sie die Caching-Dauer individuell über den Website-Header steuern, z. B. über die .htaccess-Datei oder das CMS. Sie können das Caching mit **„Disabled"** aber auch deaktivieren.

Der Mehrwert für Sie

- **Optimierte Geschwindigkeit**
  Durchschnittlich 70 Prozent höhere Geschwindigkeit Ihrer Website
- **Verfügbarkeit und Redundanz**
  Zuverlässig online – auch bei hoher Last oder Netzwerkausfällen
- **Optimale Benutzererfahrung**
  Performant, professionell und vertrauenswürdig
- **Doppelter Schutz vor DDoS-Angriffen**
  Caching von Inhalten und Blockade erkannter Überlastungsangriffe
- **Bessere Sichtbarkeit in Suchmaschinen**
  Optimierte Ladezeit für besseres Ranking

So optimieren Sie Performance und Sicherheit per CDN

1. Aktivieren Sie im Dashboard ggf. Firewall und CDN.

2. • Wählen Sie in den Firewall-Optionen unter **„Performance“** – **„Caching Level“** die passende Caching-Option aus.
   • Sucuri bietet granulare Caching-Einstellungen für die Bedürfnisse verschiedener Website-Arten:
   • **„Enabled“** (empfohlen): für statische, selten aktualisierte Websites ohne dynamische Inhalte.
   • **„Minimal Caching“**: für häufig aktualisierte Websites ohne Benutzer-Sessions, z. B. News-Portale oder Blogs.
   • **„Site Caching“**: für Websites mit Benutzer-Sessions, z. B. Webshops, Foren, geschlossene Mitglieder-Bereiche und Custom-Applikationen
   • **„Disabled“**: für interne Webseiten oder solche, die ein externes CDN nutzen.

Zum Schutz vor DDoS-Attacken werden statische Dateien unabhängig von den Cache-Einstellungen drei Tage gespeichert. Einzelne Ausnahmen definieren Sie unter **„Non-Cache URLs“**, eine komplette Deaktivierung des Cachings bietet der Developer Mode (beides ebenfalls unter **„Performance“** zu finden).

Mehr Infos:
https://docs.sucuri.net/website-firewall/performance/caching-options/
https://docs.sucuri.net/website-firewall/performance/developer-mode/

Blacklisting rückgängig machen

Wenn eine Website mit Malware infiziert ist, geben einige Internetdienste und Suchmaschinen (in den Suchergebnissen oder beim Versuch, Ihre Seite aufzurufen) Warnungen aus, dass diese Website gefährlich ist. Das kann erheblichen Schaden für Geschäft und Image des Website-Betreibers bedeuten.

Hintergrund

Technische Basis dieser Warnungen sind sogenannte **Blacklists**: Suchmaschinen oder Security-Serviceprovider analysieren automatisch Webseiten auf Anzeichen für Malwarebefall. Werden sie fündig, tragen sie die betroffenen Websites auf einer Sperrliste ein und warnen künftig vor ihrem Besuch.

Der wichtigste dieser Blacklisting-Dienste ist Google Safe Browsing. Dieser Dienst analysiert permanent die Seiten in Googles riesigem Suchindex und versorgt die Google-Plattformen (Chrome, Android, AdSense, Gmail), Provider sowie zahlreiche Browser wie Safari oder Firefox mit URL-Listen potenziell gefährlicher Webseiten. Vier Milliarden Geräte weltweit werden durch Google Safe Browsing geschützt.

Eigene Seiten entfernen lassen

Ihre Seite ist auf einer Blacklist gelandet? Wir helfen Ihnen gern.

Die Blacklist-Entfernung ist ein fester und für Sie kostenloser Bestandteil unseres Service. Das bedeutet: Wenn Sie eine Malware-Bereinigung beauftragen, kümmern wir uns automatisch auch um eventuelle Blacklist-Einträge.

So werden wir aktiv, um Blacklist-Einträge zu entfernen

Wenn wir gemäß Ihrem Auftrag Ihre Webseiten detailliert auf Kompromittierungen und Malware überprüfen, kontrollieren wir auch die 10 wichtigsten Blacklists:

- Google Safe Browsing
- Norton Safe Web
- Phish Tank
- Opera
- SiteAdvisor McAfee
- Sucuri Malware Labs
- SpamHaus DBL
- Bitdefender
- Yandex (über Sophos)
- ESET

Sollten sich Seiten von Ihnen auf einer dieser schwarzen Listen finden, setzen wir uns mit den entsprechenden Anbietern in Verbindung. Sobald wir Ihre Webseite bereinigt haben, informieren wir die Blacklist-Services darüber, dass Ihre Website gereinigt wurde und dass die Warnung entfernt werden kann. Nach Überprüfung des Antrags sollten die Warnungen verschwinden.

Wie lange dauert das Entfernen?

Wann Ihre Website von einer Blacklist gestrichen wird, hängt vom Betreiber der Liste ab. Gewöhnlich benötigen die Unternehmen drei bis fünf Arbeitstage, um Sites von ihren Blacklists zu entfernen. Google braucht in der Regel 24 bis 72 Stunden, Sucuri Malware Labs etwa vier Stunden für eine Überprüfung. Leider gibt es wenige Möglichkeiten, diesen Prozess zu beschleunigen (siehe aber unseren Kasten „Website-Blacklisting: Das können Sie tun“).

Website-Blacklisting: Tipps zum optimalen Vorgehen

1. Fordern Sie eine Malware-Bereinigung an.
2. Warten Sie, bis der Blacklist-Anbieter Ihre Website nochmals geprüft hat. Tipp: Häufig können Sie als angemeldeter Nutzer auch selbst eine Prüfung Ihrer Seiten anfordern, um diesen Prozess zu beschleunigen. Bei Google nutzen Sie dafür die Search Console bzw. die Webmaster Tools.
3. Sie können die folgenden Services nutzen, um Ihre Seiten auf weitere Blacklist-Einträge zu prüfen:
   - VirusTotal
   - Categorify
   - URLVoid

   Der Grund: Wir überprüfen nur die am häufigsten genutzten und zuverlässigsten Blacklists. Es gibt darüber hinaus einige kleinere Listenanbieter, die häufig auch fehleranfälliger sind.
4. Sollte Ihre Seite fünf Tage nach dem Säuberungsauftrag noch immer auf der Blacklist stehen, erteilen Sie bitte einen neuen Auftrag, damit wir den Fall überprüfen können.

Hinweis: Wird in den Google-Suchergebnissen bei Ihrer Seite die Warnung „Diese Website wurde möglicherweise gehackt" angezeigt, ist die Ursache kein Safe-Browsing-Blacklisting durch Malware, sondern es sind aus Google-Sicht verdächtige Aktivitäten auf der Seite. Wir beantragen auch dafür eine Überprüfung. Es kann aber bis zur Entfernung der Warnung einige Wochen dauern.

Wichtige Bereiche und Seiten wirksam absichern

Sucuri bietet eine Reihe von Möglichkeiten, sensible Seiten besonders abzusichern. Im Standard beschränkt die Sucuri Firewall den Zugriff auf Administrator-Bereiche wie /wp-admin in WordPress oder /administrator in Joomla auf autorisierte **IP-Adressen**, die Sie auf Ihre **Whitelist** gesetzt haben. So sichern Sie Ihre Website-Verwaltung, falls ein Benutzerkonto erfolgreich gehackt wurde. Sie können diese Option in den Firewall-Einstellungen deaktivieren („**Einstellungen" – „Sicherheit" – „Erweiterte Sicherheits-Optionen**").

Darüber hinaus stehen Ihnen weitere Optionen zur Verfügung, um individuelle Seiten Ihren Anforderungen gemäß abzusichern. So können Sie den Zugriff auf beliebige Seiten flexibel beschränken oder einzelne Bereiche explizit freigeben, um unerwünschte Nebenwirkungen der Firewall-Regeln zu verhindern.

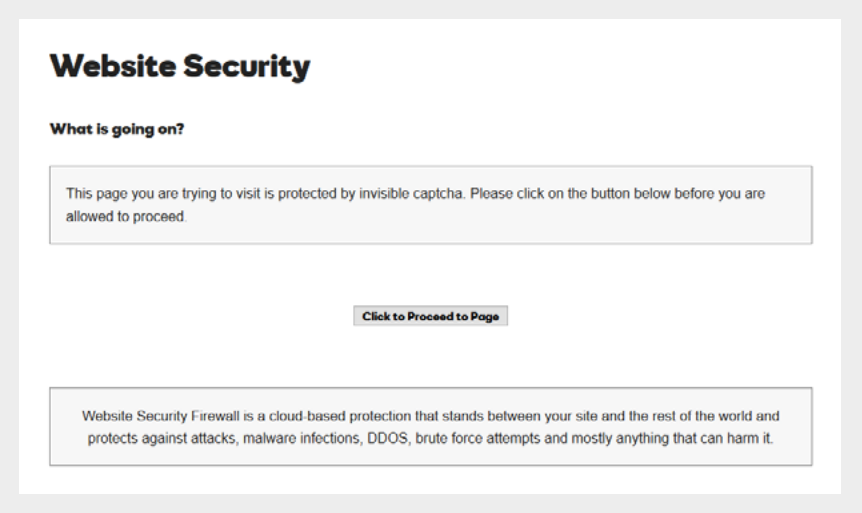
Den Zugriff auf individuelle Seiten einschränken (Protected Page)
Das "Protected-Page"-Feature soll als zusätzliche Schutzschicht sensitive Webseiten noch sicherer machen. Sie können damit den Zugriff auf bestimmte Seiten einschränken, aber auch eine sekundäre Authentifizierung für Admin-Bereiche realisieren.

Sie können eine der folgenden Authentifizierungsmethoden wählen:

- Passwortschutz
  Diese Option erzeugt ein zufälliges Passwort, das ein Benutzer bei seinem ersten Zugriff auf die geschützte Seite eingeben muss.
- IP-Adressen-Beschränkung (Whitelisting)
  Nur explizit zugelassene IP-Adressen erhalten Zugriff, alle anderen Zugriffe werden geblockt.

- **Zwei-Faktor-Authentifizierung (2FA) mit Google Authenticator**
  Diese Option fordert jeden Besucher der Seite auf, einen Code einzugeben, den die Smartphone-App Google Authenticator für kurze Zeit anzeigt. Der physische Zugriff auf das Smartphone ist damit Voraussetzung für den Zugriff auf die Seite. So kann zusätzlich zu einem normalen Passwortschutz (Faktor Wissen) ein zweiter, davon unabhängiger Schutzfaktor (Faktor Besitz) implementiert werden.

Captcha Challenge



Captchas stellen dem Besucher Aufgaben (z. B. das Erkennen von Bildinhalten), und werten die Antwort aus (Challenge-Response-Test). Damit soll sichergestellt werden, dass der Zugriff auf die Seite durch einen Menschen erfolgt und nicht durch einen Bot.

Zugriffssteuerung durch Black- und Whitelisting

Die Sucuri Firewall bietet Ihnen sehr detaillierte Möglichkeiten, bestimmte Zugriffe zu sperren (**Blacklisting**) oder alternativ Ausnahmen zu definieren, die nicht blockiert werden (Whitelisting).

Zugriffe blockieren

Sie können festgelegte IP-Adressen vom Zugriff auf Ihre Seiten ausschließen. Darüber hinaus ist es möglich, spezifische Länder entweder vom Lesezugriff oder von der Interaktion mit Ihrer Seite auszuschließen, Zugriffe bestimmter **HTTP**-Referer oder User-Agents zu blockieren sowie spezifische Cookies zu verbieten.

Zugriffe zulassen

Wenn IP-Restriktionen für den Zugriff auf geschützte Seiten (z.B. Admin-Bereiche) aktiviert sind, können Sie per Whitelisting definieren, für welche IP-Adressen, URL-Pfade, Verzeichnisse oder Dateien die Firewall-Regeln nicht angewendet werden sollen. Das kann sinnvoll sein, wenn die Firewall-Regeln dazu führen, dass der Zugriff auf bestimmte Seiten unerwünscht blockiert wird.

So schützen Sie eine wichtige Seite

Option 1: Protected Page

1. Klicken Sie im Firewall-Bereich des Dashboards auf **„Zugriffs-steuerung“** – **„Protected Page“**.
2. Geben Sie die URL der zu schützenden Seite ein (z. B. /wp-login.php). Wählen Sie eine Authentifizierungsmethode aus und klicken Sie **„Seite schützen“**.

Option 2: Einen URL-Pfad blacklisten

1. Klicken Sie im Firewall-Bereich des Dashboards auf **„URL-Pfade auf Blacklist setzen“**.
2. Geben Sie die URL der zu schützenden Seite ein (z. B. /wp-login.php) und klicken Sie **„Blacklist“**. Nur URLs auf Ihrer Whitelist können Ihre Seiten dann erreichen.

Mehr Infos:

Protected Pages:
https://docs.sucuri.net/website-firewall/whitelist-and-blacklist/protected-page/

Black- und Whitelisting:
https://docs.sucuri.net/website-firewall/whitelist-and-blacklist/

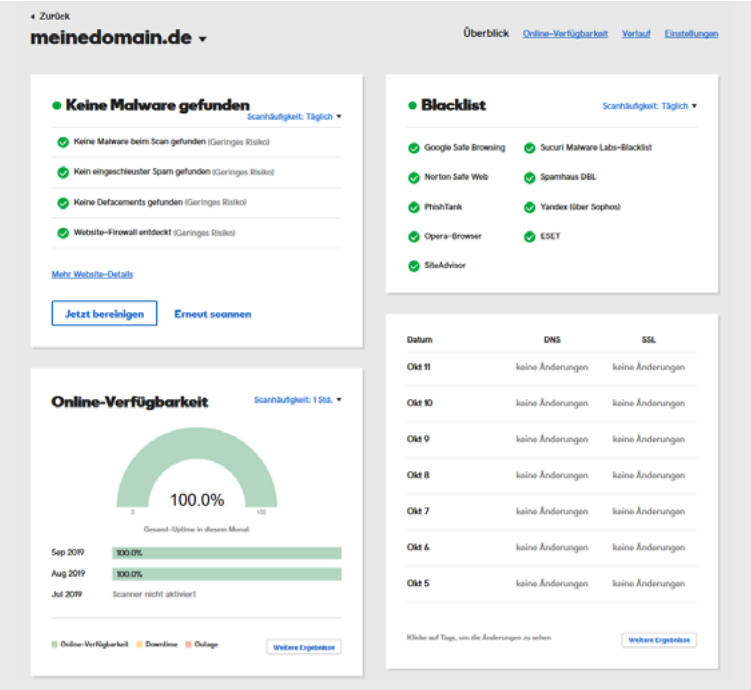
Besser informiert: Monitoring-Dashboard und Reports

Sucuri überwacht zahlreiche Aspekte Ihrer Website. Mit unseren Scannern tragen wir viele Informationen zusammen, die Ihnen helfen können, den Zustand und die Sicherheit Ihrer Seiten detailliert einzuschätzen.

Um auf diese Informationen zuzugreifen, stehen Ihnen verschiedene Möglichkeiten offen.

Sucuri-Dashboard

Die Übersichtsseite („**Overview**“) im Bereich „Website Monitoring“ zeigt den Sicherheitsstatus Ihrer Website sowie Warnungen an:



Quadrant oben links: Zeigt alle Warnungen vor Malware, injiziertem Spam oder **Defacements**.

Quadrant oben rechts: Zeigt an, ob und vom wem Ihre Website auf eine **Blacklist** gesetzt wurde.

Quadrant unten links: Zeigt, ob Ihre Website ordnungsgemäß läuft und ob es zu Ausfallzeiten oder Ausfällen gekommen ist (inkl. gewählte Scan-Frequenz).

Quadrant unten rechts: Zeigt an, ob sich Ihre DNS-Einträge und/oder Ihr SSL-Zertifikat geändert haben.

Mehr Daten zu Uptime und DNS erhalten Sie, wenn Sie jeweils auf **„More Results"** (oder oben auf **„Uptime"** bzw. **„History"**) klicken.

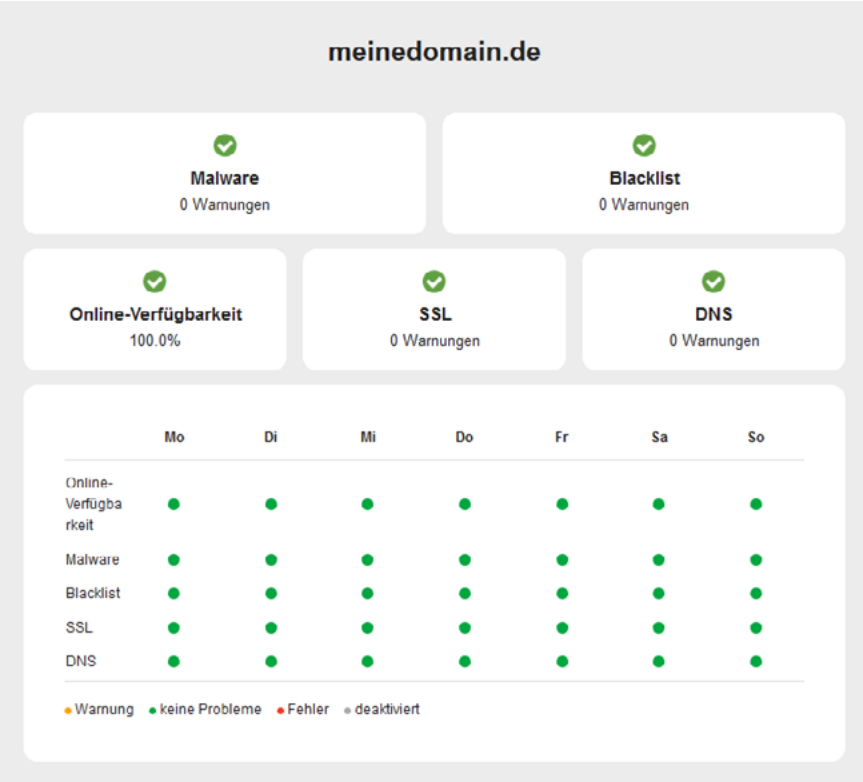
Tipp: Im Dashboard-Bereich „Website Firewall" liefert die Seite „Reports" einen detaillierten Überblick u. a. über abgewehrte Angriffe, blockierte und zugelassene Zugriffe, Besucher, Geräte und den Netzwerkverkehr.

Reports per E-Mail

Wenn Sie es bevorzugen, auf dem Laufenden zu bleiben, ohne regelmäßig das Dashboard zu überprüfen, können Sie dort unsere E-Mail-Reports aktivieren (Website Monitoring – Website – Settings – E-Mail Reports). Wählen Sie wöchentlichen oder monatlichen Versand sowie das Format Text oder PDF.

Der Report zeigt auf einen Blick, welche Scanner aktiviert sind und welche Warnungen im Berichtszeitraum ausgegeben wurden. Unter der Zusammenfassung sehen Sie den Tages- bzw. Wochenstatus der einzelnen Scanner. Der Scan-Status ist farblich gekennzeichnet:

Rot: Sofortige Aufmerksamkeit erforderlich
Gelb: Informationen geändert
Grün: Keine Probleme
Grau: Scanner deaktiviert



Wählen Sie Ihr Paket: Sucuri Website Security bei Host Europe

Mit den gestaffelten Sucuri-Paketen von Host Europe erhalten und bezahlen Sie für Ihre Websites genau den Schutz, den Sie benötigen.

Sucuri Essential

Dieses Paket bietet grundlegenden Schutz für Ihre Website (Schutzstufe 1). Es umfasst das regelmäßige Scannen Ihrer Website auf Malware, SEO-Spam und andere Kompromittierungen sowie Blacklisting und bei Bedarf die komplette Malware-Bereinigung durch unsere Experten (Reaktionszeit 12 Stunden).

Sucuri Deluxe

Zusätzlich zu den Leistungen des Essential-Pakets stehen Ihnen mit Sucuri Deluxe die Leistungen unseres **CDN** zur Verfügung: die Abwehr von Hacks und Angriffen durch die die Sucuri **Firewall** (Schutzstufe 2, S. 19) sowie optimierte Performance und Verfügbarkeit.

Sucuri Ultimate

Sucuri Ultimate umfasst alle Leistungen von Sucuri Deluxe, ergänzt durch Backup und Restore für zusätzliche Sicherheit (Schutzstufe 3) und eine verkürzte Reaktionszeit von 6 Stunden.

Sucuri Express

Soforthilfe innerhalb von 30 Minuten! Mit Sucuri Express erhalten Sie alle Leistungen von Sucuri Deluxe plus eine garantierte Reaktionszeit unserer Experten innerhalb von 30 Minuten nach Ihrem Auftrag.

Alle Sucuri-Pakete im Überblick

Sucuri Essential

Malware-Scan und -Entfernung

4,99 € / Monat

Reaktionszeit: 12 Stunden
Malware-Scan: unbegrenzt (Seiten)
Malware-Entfernung: unbegrenzt
Blacklisting: Überwachung und Beseitigung

Sucuri Deluxe

Malware-Scan und -Entfernung, Web Application

19,99 € / Monat

Reaktionszeit: 12 Stunden
Malware-Scan: unbegrenzt (Seiten)
Malware-Entfernung: unbegrenzt
Blacklisting: Überwachung und Beseitigung
Web Application Firewall (WAF)
Content Delivery Network (CDN)

Sucuri Ultimate

Alle Deluxe-Funktionen, verkürzte Reaktionszeit, Backup

29,99 € / Monat

Reaktionszeit: 6 Stunden
Malware-Scan: unbegrenzt (Seiten)
Malware-Entfernung: unbegrenzt
Blacklisting: Überwachung und Beseitigung
Web Application Firewall (WAF)
Content Delivery Network (CDN)
Backup & Restore

Sucuri Express

Alle Deluxe-Funktionen, Soforthilfe in 30 min

299,99 € / Monat

Reaktionszeit: 30 Minuten
Malware-Scan: unbegrenzt (Seiten)
Malware-Entfernung: unbegrenzt
Blacklisting: Überwachung und Beseitigung
Web Application Firewall (WAF)
Content Delivery Network (CDN)

Hier können Sie Ihr Paket bestellen:
https://www.hosteurope.de/sucuri-website-malware-scanner/

Glossar

Backdoor

Eine Backdoor (dt. „Hintertür") bezeichnet einen versteckten alternativen Zugang zu einem System, mit dem sich Sicherheitsmechanismen umgehen lassen. Die meisten Malware-Infektionen installieren solche Hintertüren (bei den 2018 von Sucuri gesäuberten Websites waren es 68 Prozent).

Blacklist

Blacklists oder dt. „schwarze Listen" sind Negativ- bzw. Sperrlisten. Im Internetbereich enthalten sie in der Regel Adressen von potenziell schädlichen Systemen. Sie können Ihre Website schützen, indem Sie bestimmte IP-Adressen „blacklisten". Ihre Website kann aber auch selbst auf die Blacklists von Security-Diensten geraten, wenn diese sie als gefährlich einschätzen, etwa nach einem Hack oder Malware-Befall.

Brute-Force-Angriff

Bei Brute-Force-Angriffen gehen Hacker mit Hilfe von Skripten oder automatisch per Bot eine große Zahl von Passwortkombinationen durch (häufig wörterbuchgestützt), um sich mit den Benutzerrechten des angegriffenen Kontos Zugang zu einem System zu verschaffen.

CDN (Content Delivery Network)

Ein Content Delivery Network (oder Content Distribution Network), kurz CDN, ist ein Netz verteilter Server-Cluster, die „Points of Presence" (PoP) genannt werden. Sie sind über das Internet verbunden und arbeiten zusammen, um Inhalte (Daten) besonders effizient und performant auszuliefern. Durch Zwischenspeicherung von Daten (Caching) auf den PoPs können Daten schneller ausgeliefert, Bandbreite eingespart und auch bei großen Lastspitzen ein optimaler Datendurchsatz gewährleistet werden.

Cross-Site Request Forgery (XSRF)

Eine Cross-Site Request Forgery, abgekürzt XSRF oder CSRF, ist ein website-übergreifender Angriff auf eine Webanwendung über den Webbrowser eines dort angemeldeten Opfers. Der Browser des angemeldeten Nutzers wird etwa durch einen untergeschobenen Link oder XSS (s. u.) dazu gebracht, eine bösartige HTTP-Anfrage zu senden mit dem Ziel, dass die Webanwendung eine Aktion ausführt, z. B. einen neuen Benutzer mit Administratorrechten anlegt.

Cross-Site Scripting (XSS)

Cross-Site Scripting (XSS) bezeichnet Angriffe, bei denen eine anfällige Webanwendung Daten, die von Nutzern manipuliert werden können (z.B. Formulardaten oder präparierte Links), ohne Prüfung auf der Webseite speichert. Beim Seitenaufruft die manipulierten Daten über den Webbrowser an den anderen Nutzer weitergesendet. Wenn diese Daten schädliche Skripte enthalten, werden diese vom Browser des Opfers ausgeführt. Kriminelle können so etwa die Benutzer-Session kapern, die Website verändern (Defacement), Phishing-Seiten ausspielen oder die Kontrolle des Browsers übernehmen.

DDoS-Angriff

DDoS („Distributed Denial of Service“) bezeichnet die gezielte Überlastung eines Servers oder eines ganzen Netzwerks, um deren Dienste funktionsunfähig zu machen („Denial of Service“ = Dienstverweigerung). Die Überlastung entsteht, weil gleichzeitig sehr viele Rechner (z. B. gekaperte PCs, Server, Router etc.) Anfragen an das Ziel senden („distributed“ = verteilt). Die CDN-basierte Sucuri WAF stellt sicher, dass bösartige Anfragen Ihren Webserver gar nicht erst erreichen – weder auf Anwendungsebene noch auf Netzwerkebene.

Defacement

Defacement, deutsch „Verunstaltung" oder „Entstellung", bezeichnet die böswillige Veränderung des Erscheinungsbilds einer Website. Hacker verschaffen sich über Sicherheitslücken oder entwendete Passwörter Zugang und verändern Texte oder Grafiken, um Website-Betreiber zu schädigen, Botschaften zu verbreiten oder ihre Reputation in Hacker-Kreisen zu erhöhen.

DNS

Das Domain Name System, kurz DNS, übernimmt in IP-basierten Netzen wie dem Internet die Namensauflösung, also die Übersetzung von Domain-Namen wie „beispiel.de" in die zugehörigen IP-Adressen.

HTTP

Das Hypertext Transfer Protocol (HTTP) ist ein Netzwerkprotokoll für die Übertragung von Daten auf der Anwendungsschicht, insbesondere für Webanwendungen. Seit 2015 gibt es HTTP in der umfassend überarbeiteten Version HTTP/2 für reduzierte Ladezeiten.

Intrusion Detection System (IDS)

Ein IDS überwacht den Datenverkehr im Netz auf verdächtige Muster (Signaturen von Angriffen) und Abweichungen von Policies oder vom Normalzustand. Dazu werden die IP-Pakete des Netzwerkverkehrs aufgezeichnet, analysiert und gefiltert. Werden Bedrohungen erkannt, wird ein Alarm ausgelöst.

Intrusion Prevention System (IPS)

IPS sind auch Intrusion Detection Systems, die aber Angriffe nicht nur erkennen, sondern auch abwehren können. Dafür können sie Datenpakete verwerfen, die Verbindung unterbrechen, Firewall-Regeln steuern oder die übertragenen Daten verändern.

IP-Adresse/Internet Protocol

Das Internet Protocol (IP) ist eines der wichtigsten Computer-Netzwerkprotokolle und die Grundlage des Internets. Vernetzten Computern werden sogenannte IP-Adressen zugewiesen, also Zahlenblöcke, die die Rechner in einem Netzwerk eindeutig identifizieren. Die Adressen ermöglichen es, Daten als IP-Pakete zwischen den Rechnern zu versenden.

Phishing

Phishing (abgeleitet von „fishing", dt. „angeln") steht für Versuche, durch Täuschung (z.B. gefälschte Webseiten oder E-Mails) an fremde Zugangsdaten und persönliche Informationen zu gelangen.

SEO-Spam

Kurz für „Search Engine Optimization Spam": Durch Einschleusung von Inhalten in fremde Webseiten versuchen Hacker, das Suchmaschinen-Ranking einer eigenen Seite zu verbessern, um z. B. mehr Werbeeinnahmen zu erzielen.

SQL-Injektion

SQL-Injektion bezeichnet das Einschleusen böswilliger Datenbankbefehle in SQL-Datenbanken (z. B. über Formulare), deren Ausführung es Hackern erlaubt, Daten zu stehlen oder zu verändern, die Kontrolle über den Server zu erlangen oder Schaden anzurichten.

Threat Intelligence

Threat Intelligence wertet große Datenmengen aus (weltweit gesammelt z. B. von der Sucuri WAF), um nützliche Informationen über aktuelle Bedrohungen und Trends zu erlangen, etwa zu laufenden Malware-Kampagnen, Angriffsstrategien und Täterprofilen.

Virtual Hardening

Das "Härten" einer Website umfasst zusätzliche Schutzmaßnahmen auf verschiedenen Ebenen (Anwendungen, Betriebssystem, Server, Datenbanken), um die Angriffsfläche zu verringern und die Sicherheit zu erhöhen. Dazu gehören beispielsweise die Deaktivierung ungenutzter Funktionen und Ports, Rechtemanagement, Zugangskontrolle (Whitelisting) oder Verschlüsselung. Beim Virtual Hardening übernimmt die Web Application Firewall entsprechende Funktionen.

Virtual Patching

Die Web Application Firewall erkennt Versuche, bekannte Sicherheitslücken auszunutzen, und schützt die dahinter liegenden Anwendungen, bis eine Systemaktualisierung eingespielt wird, die die Schwachstelle behebt. Weil der Quellcode der Anwendung nicht geändert wird, wird die Methode „Virtual Patching" genannt.

Web Application Firewall (WAF)

Eine WAF schützt Webanwendungen vor Angriffen über HTTP. Dazu entschlüsselt sie den SSL-Datenverkehr, untersucht eingehende Anfragen sowie die Antworten des Servers, analysiert JavaScript, SQL, HTML, XML, Cookies etc. und blockiert bei verdächtigen Inhalten den Zugriff. Damit schützt sie die Webanwendung u.a. vor SQL-Injektion, Cross-Site Scripting oder DDoS-Angriffen.

Whitelist

Die weiße Liste ist das Gegenstück zur Blacklist. Sie bezeichnet im Internetbereich eine Positiv- oder Ausnahmeliste mit vertrauenswürdigen Systemen. Solche Listen erleichtern den Schutz sensibler Website-Bereiche. Denn statt viele gefährliche Systeme einzeln zu identifizieren und zu blockieren, kann man so den Zugriff komplett sperren und nur für wenige vertrauenswürdige Ausnahmen zulassen.

Zero-Day-Exploit

Zero-Day-Exploits (Tag-Null-Verwertung) sind Methoden, um neu entdeckte Schwachstellen auszunutzen („Exploit"), noch bevor diese durch Aktualisierungen (Patches) beseitigt werden konnten – idealerweise noch am Tag der Entdeckung. Von Hackern entdeckte Schwachstellen werden von diesen oft lange geheim gehalten. Kriminelle, aber auch Geheimdienste sind an passenden Exploits für solche unbekannten Schwachstellen interessiert, um damit in ungeschützte Systeme eindringen zu können.

Host Europe

Sie haben weitere Fragen?

Unser Sales Team ist gerne für Sie da.

0800 626 4624

www.hosteurope.de