Whitepaper

Sucuri Website Security für Agenturen

Mehr Sicherheit für Kunden-Websites

Powered by Sucuri

Domain Factory

Inhaltsverzeichnis

Mehrwert bieten mit Sucuri

Anspruchsvolle Kunden, knappe Budgets, steigender Wettbewerbsdruck – als Internetagentur müssen Sie sich von der Konkurrenz abheben, um auch in Zukunft wettbewerbsfähig zu sein. Wie können Sie als Webdienstleister Ihren Kunden attraktive Services mit Mehrwert anbieten und gleichzeitig Aufwand und Kosten begrenzen? Die Antwort: Sucuri Website Security.

- Die Websecurity-Plattform schützt mit umfassenden und leistungsfähigen Funktionen Webseiten vor allen relevanten Cyber-Bedrohungen. Der Plattform-Betreiber Sucuri ist ein führender Anbieter von Website-Security-Lösungen und Services mit weltweiter Präsenz.
- Die Sucuri Firewall schützt Websites wirksam vor Bedrohungen aus dem Netz, von automatisierten Angriffen und DDoS-Attacken bis hin zu Zero-Day-Exploits. Mehr als 170 Millionen Angriffsversuche wurden 2019 von der Sucuri Firewall abgewehrt.
- Das Sucuris Intrusion Detection System überwacht zudem Websites auf Malware, SEO-Spam, DNS- oder SSL-Probleme und Einschränkungen der Verfügbarkeit.
- Darüber hinaus bietet Sucuri Website-Backups und Wiederherstellung und die professionelle Behebung der Folgen von Malware-Infektionen.

Kurz und knapp: Die Vorteile für Webdienstleister

1. Kunden erwarten Sicherheit

Obwohl die Nachfrage nach Website-Security steigt, können weniger als 10 Prozent der Webdienstleister ihren Kunden entsprechende Services liefern. Hinzu kommt, dass Kunden häufig nicht bereit sind, für Security-Leistungen zu zahlen, bei Problemen aber dennoch den Dienstleister verantwortlich machen.

Mit Sucuri können Sie als Agenturen Ihren Kunden von Anfang an einen Rundumschutz für deren Webseite anbieten – nicht erst, wenn es zu spät ist. Sollte dennoch Schadcode auf den Server gelangen, wird er von Sucuris Intrusion Detection System schnell und zuverlässig erkannt.

2. Schnelle und professionelle Reaktion im Schadensfall

100-prozentige Sicherheit gibt es nicht – jede Website kann gehackt werden. Eine Bereinigung im Schadensfall ist nicht nur aufwendig, sie erfordert auch spezielles Know-how und saubere Backups.

Als Sucuri-Anwender sind Sie rundum geschützt: durch jederzeit aktuelle Backups und eine schnelle, gründliche Malware-Bereinigung durch Profis. Sie als Webdienstleister müssen sich nach Auftragserteilung um nichts weiter kümmern und werde zudem stets zeitnah über den aktuellen Stand und neue Bedrohungen informiert.

3. Wirtschaftliche Lösung für Webdienstleister

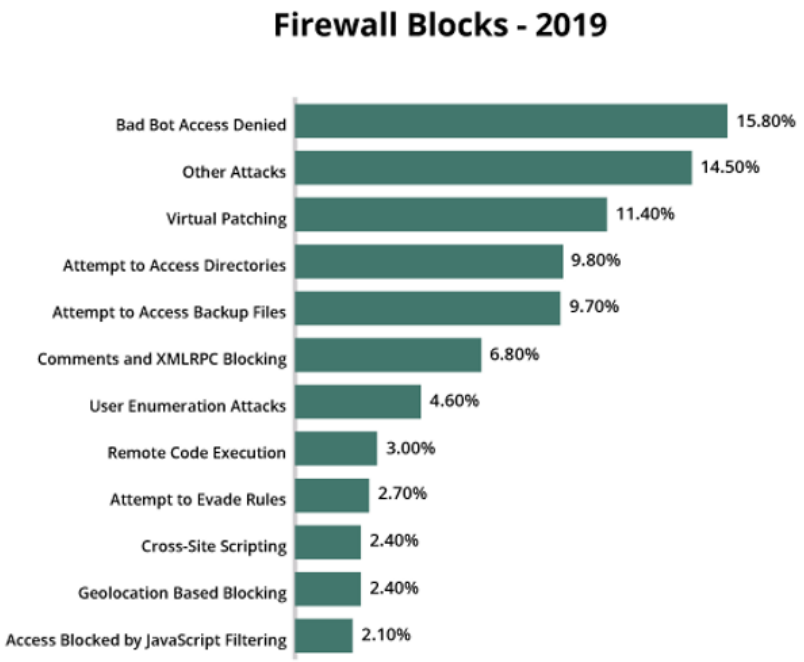
Sucuri Website Security von DomainFactory, bietet Ihnen als Agentur oder Freelancer eine kostengünstige Möglichkeit, um Kundenwebseiten zu schützen. Je mehr Websites Sie von Sucuri schützen lassen, desto wirtschaftlicher ist die Lösung für Sie.

Mehrwert Sicherheit

Cyberbedrohungen nehmen zu

Experten schätzen, dass weltweit jeden Tag mehr als 90.000 Websites gehackt werden (Quelle: Hosting Facts Internet Stats & Facts for 2019). Vor allem automatisierte Angriffe durch Bad Bots nehmen zu, die Websites auf bekannte Sicherheitslücken scannen: Täglich passiert das durchschnittlich über 60 Mal (Quelle: Sitelock Security Report 2019).
Bad Bots erzeugen heute bereits fast 22 Prozent des gesamten Webverkehrs (Quelle: Imperva Bad Bot Report 2019).

Das bestätigt auch der Sucuri Website Threat Research Report 2019, eine Analyse aller von Sucuri in 2019 abgewehrten Bedrohungen. Die Sucuri Firewall blockierte 170.827.312 Angriffsversuche – 52 Prozent mehr als im Vorjahr. Die meisten dieser Angriffe stammten von Bots.



Von der Sucuri Firewall blockierte Angriffe (Quelle: Sucuri)

Der Report zeigt auch, dass Cyberangriffe immer komplexer werden und Kriminelle massive automatisierte Kampagnen fahren, um bekannte Schwachstellen in großen wie auch kleineren Websites auszunutzen. Zu diesen Schwachstellen gehören unter anderem Sicherheitslücken in Software-Lösungen und Plugins, aber vor allem auch veraltete Systeme.

Ist ein Angriff erfolgreich, kann das für Websitebetreiber gravierende Folgen haben: Suchmaschinen zeigen als kompromittiert erkannte Seiten nicht mehr an (Blacklisting). Sicherheitswarnungen oder der Diebstahl sensibler Daten beeinträchtigen Image und Kundenvertrauen, Downtimes verursachen Umsatzeinbußen, Vertriebs- und Supportabläufe kommen ins Stocken. Zudem können gehackte Websites als Einfallstor genutzt werden, um weitere Systeme zu kompromittieren oder in das Betreiber-Netzwerk einzudringen. Von den über 60.000 infizierten Websites, die das Security Incident Response Team (SIRT) von Sucuri in 2019 bereinigt hat, fanden sich auf fast 30.000 Seiten eine oder mehrere Backdoors (Quelle: Sucuri Website Threat Research Report).

Ihre Kunden erwarten Sicherheit

Viele Kunden erwarten eine Rundumbetreuung: Sie erwarten, dass ihr Webdienstleister nicht nur die Webseite betreuen, spezielle Wünsche schnell und kostengünstig umsetzen und sich möglichst auch mit E-Commerce, SEO/SEA oder E-Mail-Marketing auskennen soll. Er soll natürlich auch für die Sicherheit der Website sorgen – aber ohne dafür teure Zusatzleistungen zu berechnen.

Angesichts der stetig wachsender Cyber-Bedrohungen ist das Thema IT- und Internetsicherheit längst im Bewusstsein von Nutzern und Unternehmen angekommen. Über 80 Prozent der Deutschen fürchten um die eigene Sicherheit im Internet (Quelle: Digitalbarometer von BSI und Polizei). Auch bei Unternehmen ist die Besorgnis über Cyber-Risiken seit 2017 deutlich gewachsen und gleichzeitig der Glaube an ihre Fähigkeit, diesen Risiken zu begegnen, gesunken (Quelle: Marsh Microsoft 2019 Global Cyber Risk Perception Survey).

Allerdings setzen die wenigsten Unternehmen selbst Cybersecurity-Maßnahmen für ihre Websites um, weil ihnen das Know-how dafür fehlt oder sie – oft stillschweigend – davon ausgehen, dass die Absicherung Bestandteil der Betreuung durch ihren Webdienstleister ist. In der Realität ist das aber selten der Fall, wie eine Umfrage unter Webdienstleistern belegt: Nur ein verschwindend geringer Teil der dort Befragten bietet überhaupt einzelne Website-Security-Services an, am ehesten noch Backups und Malware-Scans (Quelle: Sucuri Web Professional Security Survey 2019).

Security-Services von Webdienstleistern – Potenzial für Differenzierung vom Wettbewerb (Quelle: Sucuri)

Weniger als 10 Prozent der Dienstleister können Websites aktiv vor Malware-Angriffen schützen, und gerade einmal 0,24 Prozent der Dienstleister haben Website-Security und -Performance als Service im Portfolio – obwohl fast 70 Prozent sagen, dass ihre Kunden Security-Leistungen nachfragen.

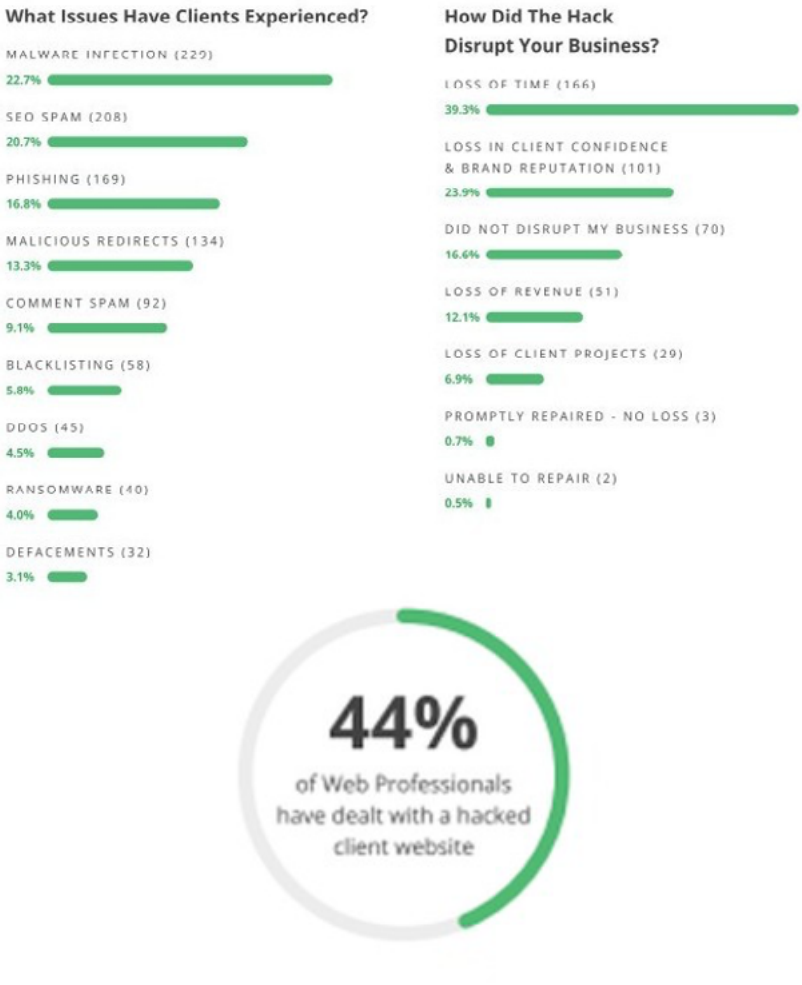
Fazit: Wenn Sie Ihren Kunden einen Rundumschutz für deren Webseiten bieten können, verschafft Sie sich damit einen Vorsprung im Wettbewerb.

Malware-Bereinigung ist aufwendig

Ähnlich verhält es sich, sollte tatsächlich die Webseite eines Ihrer Kunden kompromittiert werden. Dann ist eine schnelle Reaktion von Ihnen als Dienstleister gefragt, weil spätestens jetzt dem Kunden deutlich wird, welche Auswirkungen eine gehackte Website haben kann.

Fast die Hälfte der von Sucuri befragten Webdienstleister hatte bereits mit gehackten Kundenseiten zu tun; bei Agenturen mit mehr als 20 Kunden steigt die Wahrscheinlichkeit, mit einem erfolgreichen Hack konfrontiert zu werden, auf 55 Prozent. Häufige Folgen für die Dienstleister sind laut Studie vor allem Zeitverlust und die Beeinträchtigung der Reputation und des Kundenvertrauens, aber auch Umsatzeinbußen und verlorene Kundenprojekte.

Eine Malware-Bereinigung ist nicht nur sehr aufwendig, sie erfordert auch spezielles Know-how. Kunden sind damit in der Regel überfordert. Sie als Webdienstleister können sich natürlich das nötige Wissen aneignen, müssen dafür aber viel Zeit investieren, weil jede Malware Eigenheiten hat, die zu beachten sind.



Gehackte Kunden-Sites und ihre Folgen (Quelle:Sucuri)

Zum Beispiel fanden die Malware-Experten von Sucuri auf mehr als 5.000 infizierten Kunden-Websites die WordPress-Malware WP-VCD (Quelle: Sucuri Website Threat Research Report). Diese infiziert die functions.php aller WordPress-Themes, legt neue Admin-User an, richtet eine Backdoor zur Fernbedienung ein, spielt dubiose Werbung mit Spam-Links aus und kann sich sogar selbst neu installieren, wenn bei der Bereinigung eine einzige Datei übersehen wird.

Hinzu kommt: Infizierte Websites laufen Gefahr, auf Blacklists zu landen; vor allem bei Google. Der Dienst Google Safe Browsing identifiziert pro Woche um die 30.000 schädliche Websites. Diese werden bei der Suche nicht mehr angezeigt oder mit Warnungen wie der folgenden versehen: „Diese Website kann Ihren Computer beschädigen“. Auch andere Unternehmen pflegen solche Blacklists, darunter McAfee und Norton. Landet eine Webseite auf der Blacklist, kostet es viel Zeit und Aufwand, um diese wieder freizuschalten.

Und nicht zuletzt erfordert eine erfolgreiche Bereinigung aktuelle und saubere Backups. Wird aber der Angriff allerdings nicht rechtzeitig bemerkt, sind häufig die aktuellen Backups selbst schon infiziert.
Auch wenn Ihre Kunden nicht bereit sind, für Backups und Security-Services zu zahlen, werden sie im Schadensfall nicht selten Ihnen, als ihrem Dienstleister die Schuld zuweisen. Für Sie selbst aber rechnet sich dann der damit verbundene Arbeitsaufwand nicht mehr – ein Teufelskreis.
Mit Sucuri Website Security lösen Sie als Agenturen all diese Probleme auf einen Schlag und können Ihren Kunden einen Mehrwert bieten, mit dem Sie sich von Ihren Mitbewerbern differenzieren können.

Beispiele aus der Praxis

Szenario 1: Kunden-Website schützen

Einer Ihrer Kunden liest eine aktuelle Schlagzeile über DDoS-Angriffe, die an Intensität und globaler Verbreitung exponentiell zunehmen, Webdienste tagelang lahmlegen und häufig mit Erpressung einhergehen. Auf demselben Portal findet er Nachrichten über Datendiebstähle, SEO-Spam, Bad Bots und „Attacks as a Service“. Sehr beunruhigt fragt er bei Ihnen an, ob seine Website sicher ist.

Die Folgen ohne Sucuri

Sie als Webdienstleister erklären Ihrem Kunden, dass die Absicherung einer Website permanenter Anstrengungen bedarf und aufwendig ist. Sie empfehlen u. a. regelmäßige Backups, Updates und Malware-Scans, starke Passwörter, restriktive Zugriffsrechte, Verzicht auf nicht unbedingt nötige Anwendungen und Erweiterungen sowie Validierung und Bereinigung von Benutzereingaben. Der Kunde kann das nicht alles selbst leisten, hat aber auch kein Budget, um Sie damit zu beauftragen. Deshalb weist der Kunde eventuell einen seiner Mitarbeiter an, den Markt zu sondieren, um einen anderen Webdienstleister zu finden, der Security als Inklusivleistung anbietet.

Die Lösung mit Sucuri

Sie als Webdienstleister erklären dem Kunden, dass seine Website sicher ist: Sucuri Website Security sorgt für den professionellen Schutz vor Hackern, Malware, Datenverlusten, DDoS- und Brute-Force-Angriffen oder Zero-Day-Exploits. Mehr noch: Mit dem Sucuri Vertrauenssiegel kann Ihr Kunde das auch seinen Websitebesuchern zeigen und so sein Image stärken.

Das Intrusion Detection System von Sucuri überwacht regelmäßig die Webseite Ihres Kunden auf Anzeichen für Kompromittierungen (Indicators of Compromise), etwa einen Malware-Befall, z.B. aufgrund eines unsicheren Plugins oder eines schlecht gesicherten Admin-Zugangs. Werden Anzeichen für eine Schadsoftware gefunden oder verdächtige Aktivitäten registriert, werden Sie als Webdienstleister sofort informiert und können bei Sucuri eine Bereinigung anfordern.

Darüber hinaus bietet die Sucuri Firewall einen Echtzeit-Schutz vor verschiedensten Bedrohungen, und das sowohl für Anwendungen (Web Application Firewall) als auch auf Netzwerkebene. Dafür nutzt Sucuri ein weltweit verteiltes Content-Delivery-Network (CDN) und überwacht als Proxy den Netzwerkverkehr über HTTP und HTTPS. Das CDN und die Sucuri-eigenen DNS-Dienste sorgen für bessere Performance und Verfügbarkeit der Website.

Abgerundet wird die Sucuri-Absicherung durch automatische Backups, mit deren Hilfe im Ernstfall ein beliebiger Stand aus den vergangenen drei Monaten wiederhergestellt werden kann – mit wenigen Mausklicks über das Sucuri Dashboard.

Ihr Kunde ist beruhigt und zufrieden. Denn er ist vor Cyber-Bedrohungen gut geschützt – und er weiß jetzt auch, warum seine Webseite bei den Performance-Tests von Google PageSpeed Insights besser abschneidet.

Szenario 2: Auf Sicherheitsvorfall richtig reagieren

Einer Ihrer Kunden installiert in seiner TYPO3-Installation eine populäre Erweiterung, die eine kritische Schwachstelle aufweist: Sie erlaubt einem nicht authentisierten Angreifer die Remote-Ausführung von SQL-Injection-Angriffen. Die Schwachstelle wird von Kriminellen entdeckt, aber geheim gehalten und daher nicht geschlossen (Zero-Day-Exploit).

Die Folgen ohne Sucuri

Weil die Extension Benutzereingaben – zum Beispiel in einem Formular – nicht korrekt prüft und bereinigt, können Hacker darüber böswillige SQL-Kommandos einschleusen und ausführen. So gelingt es den Kriminellen, Zugangsdaten für ein Admin-Konto des Kunden auszulesen und seine Webseite mit SEO-Spam-Code zu infizieren. Unter anderem verteilen sie auf den Seiten z.B. Keywords wie „viagra“, „cialis“ und „tadalafil“ und legen auf dem Server verschiedene Dateien ab, mit deren Hilfe Suchmaschinennutzer auf dubiose Online-Apotheken weitergeleitet sowie Spam-E-Mails verschickt werden.

TYPO3 ist etwa im Vergleich zu WordPress seltener von Malware betroffen, sodass auf Kundenseite niemand mit einem Vorfall wie diesem rechnet. Lange Zeit bleibt der Angriff unentdeckt, weil die Seite für normale Besucher unverändert aussieht – der SEO-Spam-Code ist nur für Suchmaschinen-Bots sichtbar. Bald erscheinen die Seiten bei Google-Suchen nach Viagra und Co. auf den vorderen Rängen; wer auf die entsprechenden Links klickt, landet allerdings bei einer Online-Apotheke.

Nach einiger Zeit wird die komplette Domain auf Googles Blacklist gesetzt. Der Webtraffic bricht ein, immer mehr Kunden fragen nach, was los sei. Der Kunde sieht das Kundenvertrauen und sein Image erheblich gefährdet,

und alarmiert Sie als Webdienstleister und fordert schnellstmöglich Hilfe. Sie als Dienstleister beauftragen daraufhin einen Dritten mit der Behebung der Infektion, weil Ihnen dafür zum Beispiel selbst die Ressourcen fehlen. Eine häufige Konsequenz: erst mehrere Wochen nach dem Hack wird die Webseite bereinigt – der Kunde aber weigert sich, den entstandenen Aufwand zu ersetzen.

Die Lösung mit Sucuri

Dank regelmäßiger Malware-Scans erkennt Sucuri schon bald nach dem Hacker-Angriff die Infektion und benachrichtigt Sie als Webdienstleister. Sie beauftragen sofort Sucuri mit der Bereinigung der Website und können sich dann entspannt zurücklehnen.

Für die Security-Profis ist der Fall zunächst Routine: In 2019 waren 62 Prozent der von Sucuri bereinigten Websites mit SEO-Spam infiziert. Bei näherer Inspektion finden sie aber zusätzlich zum SEO-Spam auch eine Backdoor und Fernsteuerungsmöglichkeiten, mit denen die Kriminellen noch größeren Schaden anrichten könnten. Anhand der Logfiles erkennen die Experten von Sucuri den genauen Zeitpunkt der Infektion und stellen mit Hilfe der von Sucuri angelegten Backups eine saubere Installation wieder her. Zudem sorgen sie dafür, dass sämtliche Blacklistings rückgängig gemacht werden.

Dann gleichen sie die installierten TYPO3-Extensions mit Sucuris Vulnerability-Datenbank ab, um die Quelle der Infektion ausfindig zu machen. Zwei Millionen SQLI-Angriffe blockt die Sucuri Firewall pro Jahr – aber absolute Sicherheit gibt es auch hier nicht, gerade bei Zero-Day-Attacken. Bis zum Erscheinen eines Updates für die Extension kann die beschriebene Sicherheitslücke zum Beispiel per Virtual Patching geschlossen werden.

Sicherheitsfunktionen von Sucuri

Intrusion Detection: Malware-Scans, Bereinigung und Blacklisting-Schutz

Sucuri überprüft regelmäßig alle Webseiten auf Anzeichen für Kompromittierungen (Indicators of Compromise, IOC) und informiert bei Problemen den Betreiber oder Sie als Agentur.

Überwachung

- Malware-Infektionen (Remote & Server Side Scans)
- Website-Verfügbarkeit
- SEO-Spam
- Blacklist-Status
- SSL-Zertifikate
- DNS-Einstellungen

Professionelle Reaktion

- Sorgfältige Reparatur durch erfahrene Analysten
- Wiederherstellung der vollen Funktionsfähigkeit
- Nachhaltige Bereinigung aller Webseiten
- Entfernen von Malware, Backdoors und SEO-Spam
- Gestützt auf umfassende Threat Intelligence
- Rückgängigmachen von sämtlichen Blacklistings
- Schnelle Reaktion – nach 30 Minuten im Tarif „Express“

Sucuri Firewall: Schutz von Anwendungen und Netzwerk

Die Sucuri Firewall schützt Websites vorbeugend vor Malware und Hacker-Attacken. Basierend auf einem global verteilten, leistungsfähigen Content Delivery Network, filtert die Firewall den Netzwerkverkehr und blockiert bösartige Anfragen, bevor diese den Server erreichen.

Vorbeugender Schutz

- Abwehr von Malware- und Hacker-Angriffen
- Schutz vor Zero-Day-Exploits
- Blockade von DDoS-Attacken
- bwehr von Brute-Force-Attacken
- Virtual Patching & Hardening
- Besonderer Schutz kritischer Seiten
- Geoblocking

Optimierte Verfügbarkeit und Performance

- Caching von statischem Webcontent auf allen CDN-Knoten weltweit
- Beschleunigung durch weniger Datenbankabfragen
- Kürzere Laufwege zwischen Client und auslieferndem Server
- Schutz vor Ausfällen und Leistungsbeeinträchtigungen

Backups: Sicherung und Wiederherstellung

Auf Wunsch speichert der Backup-Service von Sucuri 90 Tage lang sämtliche Website-Dateien und Datenbanken außerhalb der Hosting-Infrastruktur und unerreichbar für Hacker und Malware. So kann im Notfall – z. B. nach einer Bereinigung oder einem Defekt – mit wenigen Mausklicks eine funktionsfähige Version wiederhergestellt werden.

Für den Notfall gerüstet

- Automatische Backups für 90 Tage
- Täglich, wöchentlich, monatlich
- Hochsichere Infrastruktur
- Exakte und komplette Wiederherstellung einer sauberen Installation

Sucuri Website Security: Pakete

Angebote für verschiedene Sicherheitsanforderungen

DomainFactory bündelt die Services von Sucuri Website Security in vier unterschiedlichen Paketen. So können Sie als Agentur Ihren Kunden flexibel die Sicherheit anbieten, die Ihre Kunden tatsächlich brauchen.

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