

Schnelleinstieg Sucuri



INHALT

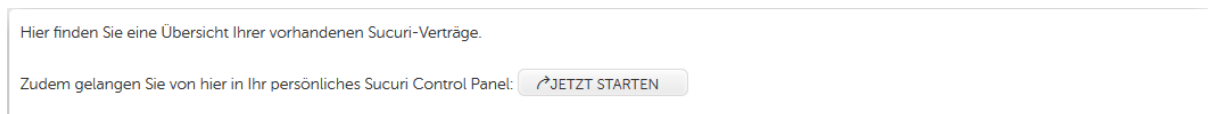
SCHNELLEINSTIEG SUCURI	1
WAS IST SUCURI?	3
WIE RICHTE ICH SUCURI EIN?	3
ERKLÄRUNG DER MENÜPUNKTE	4
Monitoring: Überblick.....	4
Monitoring: Online-Verfügbarkeit.....	6
Monitoring: Verlauf.....	6
Monitoring: Einstellungen.....	7
Firewall: Aktivierung.....	9
Firewall: Berichte.....	10
Firewall: Audit Trails	10
Firewall: Echtzeit	10
Firewall: Einstellungen	11
Backups	12
Backups: Einstellungen.....	13
Säubern: Malware Removal Requests	14
Säubern: Produkt Support	15

Was ist Sucuri?

Sucuri ist ein 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 zu schützen.

Wie richte ich Sucuri ein?

Im KIS wählen Sie den Produktbereich Sucuri und anschließend wählen Sie „Jetzt Starten“:



Es öffnet sich nun ein neues Fenster und Sie können Ihr Sucuri Paket einrichten:



Nun werden Sie aufgefordert, anzugeben, ob Ihre Domain bei Host Europe/GoDaddy registriert ist oder bei einem anderen Anbieter:

Wie möchtest du anfangen?

Wir helfen dir, um die Einrichtung in nur wenigen Schritten durchzuführen.



Auf der nächsten Seite können Sie Ihre Domain eingeben:

Wie lautet die URL deiner Website?

Nachdem Sie die Domain erfolgreich eingerichtet haben, können Sie das Paket verwalten. In der ersten Übersicht der Verwaltung sehen Sie zuerst die Meldung:

„Website gerade hinzugefügt, niemals geprüft“

Die Malware Prüfung erfolgt automatisch und ist nach einigen Stunden abgeschlossen. Sobald die erste Prüfung erfolgt ist, können Sie unter „Einstellungen - Monitoring-Arten“ weitere Prüfungen wie Online-Verfügbarkeit/DNS/SSL aktivieren.

Wenn die Malware Prüfung Auffälligkeiten auf ihrer Webseite feststellt, werden Sie per E-Mail benachrichtigt. Anschließend sollten Sie eine Anfrage zur Bereinigung unter dem Punkt „Aufräumen“ einreichen. Weitere Informationen dazu finden Sie auf Seite 12.

Erklärung der Menüpunkte

Monitoring: Überblick

Wenn Sie alle Prüfungen aktiviert haben (siehe Monitoring: Einstellungen) sehen Sie folgende Übersicht:

The screenshot shows the Host Europe monitoring dashboard. It is divided into several sections:

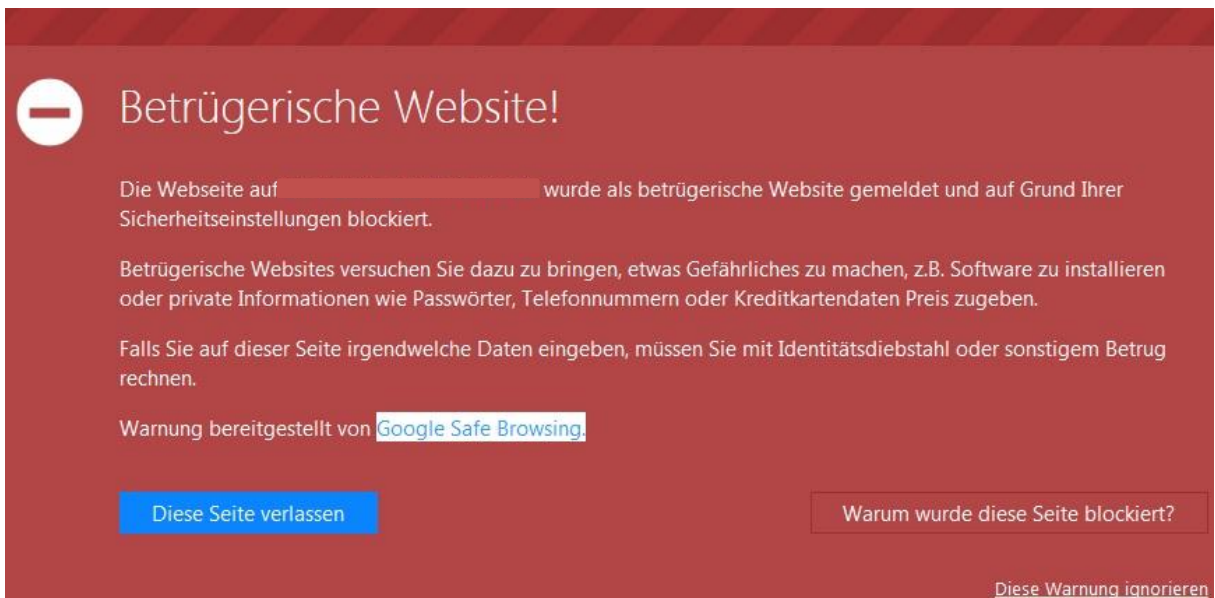
- Keine Malware gefunden** (Scanhäufigkeit: Täglich): A list of scan results with green checkmarks indicating no malware, spam, or defacements were found. A yellow warning icon indicates a website firewall was found. A button labeled "Jetzt bereinigen" (1) is highlighted.
- Blacklist** (Scanhäufigkeit: Täglich): A list of blacklist checks with green checkmarks, including Google Safe Browsing, Norton Safe Web, PhishTank, Opera-Browser, SiteAdvisor, Sucuri Malware Labs-Blacklist, Spamhaus DBL, Yandex (über Sophos), and ESET. A red circle with the number "2" is around this section.
- Online-Verfügbarkeit** (Scanhäufigkeit: 1 Std.): A gauge showing 100.0% uptime. Below the gauge, a table shows scanner status for previous months (Jul 2019, Jun 2019, Mai 2019) as "Scanner nicht aktiviert". A red circle with the number "3" is around this section.
- DNS and SSL**: A table showing the status of DNS and SSL checks over time. A red circle with the number "4" is around this table.

Datum	DNS	SSL
Aug 4	aktuell	-
Aug 3	-	-
Aug 2	-	-
Aug 1	-	-
Jul 31	-	-
Jul 30	-	-
Jul 29	-	-

1. Hier erhalten Sie eine Auflistung über den Status der letzten Überprüfungen(Scans).
 - Malware (eingeschleustes Schadprogramm/Schadcode)
 - eingeschleuster SEO Spam (Schlagwörter und eingeschleuste Verlinkungen)
 - Defacements („Verunstaltung“ unberechtigtes Verändern einer Website)
 - Website-Firewall (Schützt die Webseite vor Angriffen wie z.B. DDoS)

Mit „Jetzt bereinigen“, können Sie eine manuelle Anfrage zur Malware Bereinigung einreichen. Mit „Erneut scannen“, wird ein Auftrag in die Warteschlange gelegt, der Scan erfolgt so bald wie möglich.

2. Bei der Auflistung der Blacklists erkennen Sie, ob Ihre Seite bereits als Verdächtig eingestuft worden ist. Sollte Ihre Seite z.B. bei „Google Safe Browsing“ gelistet sein, wird beim Aufruf Ihrer Seite in den gängigsten Browsern eine Warnmeldung angezeigt.



Betrügerische Website!

Die Webseite auf [redacted] wurde als betrügerische Website gemeldet und auf Grund Ihrer Sicherheitseinstellungen blockiert.

Betrügerische Websites versuchen Sie dazu zu bringen, etwas Gefährliches zu machen, z.B. Software zu installieren oder private Informationen wie Passwörter, Telefonnummern oder Kreditkartendaten Preis zugeben.

Falls Sie auf dieser Seite irgendwelche Daten eingeben, müssen Sie mit Identitätsdiebstahl oder sonstigem Betrug rechnen.

Warnung bereitgestellt von [Google Safe Browsing](#)

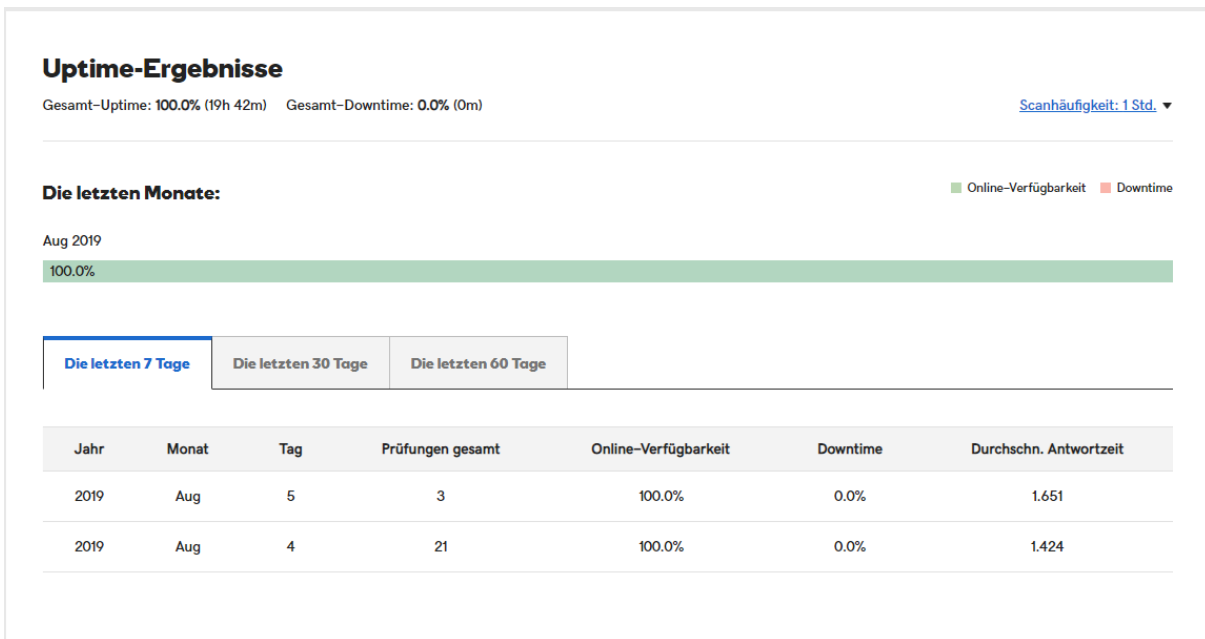
[Diese Seite verlassen](#) [Warum wurde diese Seite blockiert?](#)

[Diese Warnung ignorieren](#)

3. Die Online-Verfügbarkeit prüft im eingestellten Intervall, ob die Seite über „http/s“ erreichbar ist und informiert Sie per Mail, sobald eine Nichterreichbarkeit festgestellt wird
4. In dieser Übersicht finden Sie den Status zu DNS- und SSL-Änderungen. Beim DNS werden Sie z.B. informiert, sobald sich die IP Ihrer Domain ändert. Für SSL-Zertifikate, werden Änderungen an den Zertifikatsdaten wie z.B. der Signatur selbst beobachtet.

Monitoring: Online-Verfügbarkeit

Die Online-Verfügbarkeit zeigt Prozentual an, wie lange die Webseite erreichbar und nicht erreichbar war.



Monitoring: Verlauf

Im Verlauf sehen Sie, wann Ihre Seite z.B. mit Malware infiziert oder auf einer Blacklist war.

[Die letzten 7 Tage](#)
[Die letzten 30 Tage](#)
[Die letzten 60 Tage](#)

Datum	Website	Blacklist	DNS
Aug 5	✓	✓	-
Aug 4	▼	✓	<input type="button" value="aktuell"/>

Monitoring: Einstellungen

Bei den Monitoring-Arten können Sie bestimmen, welche Scans aktiv sein sollen. Außerdem können Sie hier die Häufigkeit der Scans konfigurieren.

Monitoring-Arten	E-Mail-Berichte	Trust Seals
Malware + Blacklist Aktiviert vor: 11 Stunden	Täglich ▼	
DNS	Täglich ▼	<input checked="" type="checkbox"/>
SSL	Täglich ▼	<input checked="" type="checkbox"/>
Online-Verfügbarkeit	Jede Stunde ▼	<input checked="" type="checkbox"/>

Sie können einen E-Mail-Bericht aktivieren und diesen z.B. so einstellen, dass Sie wöchentlich eine Übersicht aller Überprüfungen erhalten.



Monitoring-Arten	E-Mail-Berichte	Trust Seals
	<input checked="" type="checkbox"/> E-Mail-Berichte aktivieren ?	
Häufigkeit:	Typ:	
Wöchentlich ▼	HTML ▼	

Mit dem Trust-Seal können Sie ein Siegel auf Ihrer Webseite einbinden und damit dem Besucher zeigen, dass Ihre Webseite Sucuri verwendet bzw. verifiziert und gesichert ist.

[Monitoring-Arten](#) [E-Mail-Berichte](#) **Trust Seals**

Trust Seals aktivieren ?

Farbe wählen

Stil wählen

Rechts ▼ Code generieren

Firewall: Aktivierung

Für die Aktivierung der Firewall müssen Sie die Firewall-IP für Ihre Domain in Ihren DNS-Einstellungen hinterlegen. Anschließend dauert es bis zu 24 Stunden, bis die neue IP-Adresse von Sucuri erkannt wird und die Firewall aktiviert werden kann.

The image shows two side-by-side screenshots of the Host Europe firewall management interface for the domain 'beispiel-domain.de'. The left screenshot, labeled 'Firewall deaktiviert', shows the domain name, Hosting-IP (123.123.123.101), and Firewall IP (101.121.121.121). The status is 'Firewall deaktiviert' in red. A green 'Aktivieren' button is visible. Below are links for 'Berichte', 'Audit Trails', and 'Clear Cache'. The right screenshot, labeled 'Firewall aktiviert', shows the same information but with a gear icon in the top right. The status is 'Firewall aktiviert'. Below the links, there is a bar chart showing 0 blocked and 117 allowed connections. The links 'Berichte', 'Audit Trails', 'Clear Cache', and 'IP-Zugriffssteuerung' are also present.

Feature	Value
Blockiert	0
Zugelassen	117

Firewall deaktiviert

Firewall aktiviert

Firewall: Berichte

Im Bericht finden Sie eine Analyse der Zugriffe wie z.B. Anfragen nach Land sortiert oder die Zugriffe pro Stunde. Diesen Bericht können Sie sich auch per E-Mail zusenden lassen, damit haben Sie eine bessere Übersicht über die Anfragen auf Ihrer Webseite.

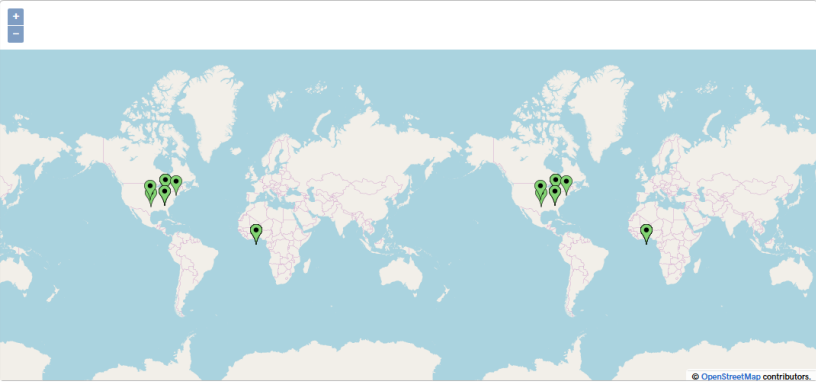
Firewall: Audit Trails

Die Audit Trails bieten Ihnen Details zu den blockierten Anfragen. Hier sehen Sie ob die Anfrage z.B. als Bot erkannt wurde und welcher Pfad aufgerufen wurde.

Firewall: Echtzeit

In der Echtzeit Übersicht sehen Sie alle aktuell eingehenden Anfragen auf Ihre Webseite. Bei Auswahl einer einzelnen Anfrage erhalten Sie weitere Details. Anschließend können Sie die IP-Adresse oder den aufgerufenen Pfad auf die Whitelist (immer zulassen) oder auf die Blacklist (immer blockieren) setzen.

Protokolle filtern nach: Alle Anfragen Zugelassene Anfragen Blockierte Anfragen Aktualisieren



IP-Adresse	Ressourcen-Pfad	HTTP-User-Agent	Datum/Uhrzeit
2600:1f14:b62:9e02:e607:645b:fea7:4687	GET /	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.109 Safari/537.36	03/Sep/2019:03:15:44 -0400
2600:1f14:b62:9e03:a00:2d37:957a:c908	GET /	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.109 Safari/537.36	03/Sep/2019:03:20:20 -0400

Anfragenübersicht

Ressourcen-Pfad: Whitelist Blacklist /

IP-Adresse: Whitelist Blacklist 2600:1f14:b62:9e02:e607:645b:fea7:4687

Reverse IP: 2600:1f14:b62:9e02:e607:645b:fea7:4687

Anfragemethode: GET

HTTP-Protokoll: HTTP/1.1

HTTP-Status: 200

HTTP-Referer: (no referer)

HTTP-User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)...

Datum/Uhrzeit (GMT): 03/Sep/2019:03:15:44 -0400

Firewall: Einstellungen

In den Einstellungen finden Sie sehr viele Informationen und Konfigurationsmöglichkeiten. Die meisten Punkte sind hier bereits ausführlich erklärt, bei einigen finden Sie auch das „?“ Symbol für weitere Informationen. Daher werden die einzelnen Punkte hier nicht im Detail beschrieben.

Im Allgemeinen Bereich sehen Sie z.B. eine Übersicht der aktuellen Firewall Konfiguration oder können weitere Server als Backupserver hinzufügen.

The screenshot shows the Host Europe control panel for Firewall settings. The 'Allgemein' (General) tab is selected. A green status bar at the top indicates 'Service ist aktiviert' (Service is active) and shows the domain 'he-mitarbeiter.schule' pointing to IP '192.124.249.54'. Below this, configuration details are listed: Domain: he-mitarbeiter.schule, Kontopakete: ultimate, Hosting-IP-Adresse: 178.77.108.140, and Firewall-IP-Adresse: 192.124.249.54. A tooltip is displayed over the Firewall-IP-Adresse field, providing instructions: 'Wenn auf deinem Hosting-Server eine Firewall wie CSF oder ModSecurity aktiviert ist, empfehlen wir, dass du unsere IP-Adressen auf deine Whitelist setzt. Da alle Verbindungen zu unserem Hosting-Server über unsere Firewall gehen, verhindert das Whitelisten unserer IP-Adressen, dass wir fälschlicherweise blockiert werden.' A red arrow points to a question mark icon next to the 'Firewall-IP-Adressen auflisten (für Whitelist)' dropdown menu. To the right, there is a 'Screenshot' section with a small image placeholder.

Über die Zugriffsteuerung können Sie IPs/URLs oder User-Agents blockieren oder auf die Whitelist setzen.

Außerdem können Sie hier ganze Länder aussperren (Geo-Blockierung).

Im Bereich Sicherheit haben Sie erweiterte Optionen zum Schutz Ihrer Webseite. Hier können Sie die Sicherheitsstufe erhöhen oder zusätzliche Sicherheitsheader aktivieren.

Unter HTTPS/SSL verwalten Sie die Umleitung auf HTTPS und das SSL-Zertifikat.

Im Bereich Performance können Sie das Verhalten des Cache konfigurieren.

Sie können hier auch einzelne IP-Adresse vom Caching ausschließen, wenn Sie z.B. Änderungen an der Seite vornehmen und diese sofort überprüfen möchten.

Die API bietet die Möglichkeit über ein Skript die Konfiguration der Firewall zu steuern und z.B. ohne Login in das Dashboard den Cache zu leeren. Dies ist z.B. für Entwickler und fortgeschrittene Nutzer interessant.

Backups

Die Backup-Funktion sichert Ihre Webseite über einen FTP/SFTP Zugang. Die Datenbank wird über einen direkten Zugriff oder PHP-Skript gesichert, welches lokal auf dem Server abgelegt wird. Für die Datenbank und den FTP Zugriff müssen Sie die entsprechenden Zugangsdaten manuell hinterlegen.

In der Übersicht sehen Sie den Status der letzten Backups.

Außerdem können Sie ein Backup sofort anstoßen und den Zeitpunkt der automatischen Backups definieren.

Für eine Wiederherstellung wählen Sie beim gewünschte Datum den Punkt „Wiederherstellungsoptionen“. Hier können Sie die Dateien/Datenbank automatisch wiederherstellen lassen oder als ZIP herunterladen. Bei der automaischen Wiederherstellung werden die bestehenden Daten ersetzt. Es werden jedoch keine neuen Daten gelöscht die im Backup noch nicht vorhanden sind.

Sollte ein Backup fehlschlagen, können Sie sich in den Backup-Details den genauen Fehler anzeigen lassen.

Letztes Backup erfolgreich

03 Sep 2019

Nächstes Backup

in 23h 54m

Jetzt sichern

Backup-Häufigkeit:

Täglich

Startzeit des Backups (UTC):

12:00

Benachrichtigungen:

Nach jedem Backup

Jun 2019

Jul 2019

Aug 2019

Sep 2019

Datum	Status	Dateien hinzugefügt	Dateien entfernt	Dateien geändert	Details	Aktion
03 Sep	Backup abgeschlossen! (keine Datenbank)	0	0	4	Backup-Details	<div style="background-color: #007bff; color: white; padding: 5px 10px; border-radius: 3px; width: 100px; margin: 0 auto;">Wiederherstellungsoptionen</div>
01 Sep	Backup fehlgeschlagen!	-	-	-	Backup-Details	<div style="background-color: #add8e6; padding: 5px 10px; border-radius: 3px; width: 100px; margin: 0 auto;">Wiederherstellungsoptionen</div>

Backups: Einstellungen

In den Website-Details können Sie die Zugangsdaten für den S/FTP-Zugang hinterlegen und anpassen. Die SFTP-Methode benötigt einen SSH Zugang.

Bei den Datenbankoptionen ist es wichtig die manuelle Konfiguration auszuwählen, da sonst keine Verbindung zur Datenbank möglich ist.

Anschließend fügen Sie die gewünschte Datenbank hinzu:

Neue Datenbank hinzufügen

Datenbankname:

Datenbank-Benutzername: Datenbank-Passwort:

Datenbank-Host: Port:

Verbindungstyp:

Direkt zu MySQL Lokaler Einsatz von PHP

Eine PHP-Datei wird dann über FTP auf deinen Server hochgeladen und abgerufen, um das Datenbank-Backup zu erstellen. Verwende diese Option nur, wenn keine direkte Verbindung zu MySQL möglich ist.

Bei dem Verbindungstyp wählen Sie „Lokaler Einsatz von PHP“ damit der Zugriff auf die Datenbank lokal auf dem Server erfolgt.

Alternativ können Sie den externen Zugriff für die Datenbank erlauben, dann funktioniert die automatische Erkennung bei bekannten CMS wie Wordpress und es werden keine weiteren Daten benötigt.

Unter Weitere-Optionen können Sie das Backup Intervall konfigurieren.

Außerdem können Sie hier Verzeichnisse hinzufügen die von Backup ausgeschlossen werden sollen. Dies können z.B. Verzeichnisse sein wo Daten nur temporär abgelegt werden, wie z.B. ein Cache-Verzeichnis

Säubern: Malware Removal Requests

Sie sehen hier eine Übersicht aller Anfragen bzw. offener Tickets und deren Status. Außerdem können Sie hier einen neuen Vorgang zur Entfernung von Malware und anderen unerwünschten Inhalten eröffnen. Dafür gehen Sie auf „Neue Malware Removal Request“ und wählen anschließend die betroffene Domain und die zutreffenden Punkte aus.

The screenshot shows a navigation bar with three tabs: "Malware Removal Requests" (active), "Produkt Support", and "FAQ". To the right is a blue button labeled "Neue Malware Removal Request". Below the navigation is a search bar with the placeholder text "Suche nach einem Ticket hier ..." and a "Suche" button. The main content area displays the message "Sie haben keine malware-Entfernungsanfragen erstellt" (You have not created any malware removal requests) and a sub-message: "Tickets, die du erschaffst, erscheinen auf dieser Seite. Bitte erstellen Sie zuerst einen malware-Entfernungsanfragen." (Tickets you create appear on this page. Please create a malware removal request first). A blue button labeled "Nachrichten Malware Removal Request" is centered below the text.

Malware Removal Request

Bitte verwenden Sie dieses Formular, um eine Malware-Entfernung (Cleanup) auf Ihrer Website anzufordern. Je nach Komplexität des Falles kann es einige Stunden dauern.

Infizierte Seite:

Ich habe Probleme mit:

- Meine Website ist auf der schwarzen Liste
- Es gibt eine Warnung über meine Website bei Google
- Erhalten eine Malware-Warnung bei Google Webmaster-Tools
- Erhielt eine Warnung von der Überwachung
- Sitecheck sagt, dass es ein Problem mit meiner Website gibt
- Meine Website sendet E-Mails auf eigene Faust
- Mein Hosting-Provider hat meine Website wegen Malware heruntergefa
- Ich sehe seltsame Dateien und / oder Ordner

Säubern: Produkt Support

Wenn Sie eine Frage zu Sucuri haben, können Sie ein Ticket unter „Produkt Support“ öffnen. Hier können Sie z.B. allgemeine Fragen zur Firewall stellen oder Probleme bei der Einrichtung klären.

Malware Removal Requests **Produkt Support** FAQ [Neues Ticket](#)

Suche nach einem Ticket hier ...

Sie haben keine Karten erstellt

Tickets, die du erschaffst, erscheinen auf dieser Seite. Bitte erstellen Sie zuerst einen Karten.

[Nachrichten Ticket](#)

Neues Support-Ticket

Bezüglich:

Ich habe Probleme mit:

Firewall Website

Ihre technische Kompetenz:

Fach:

Details: