Host Europe

# Website Security powered by Sucuri

So optimieren Sie Sicherheit, Verfügbarkeit
und Performance für Ihre Websites

E-Book Teil 1

# Inhaltsverzeichnis

# Sucuri Website Security: Sicherheit und Performance für Ihre Webseiten

Webpräsenzen zu managen bringt viel Arbeit und auch große Verantwortung mit sich. Website-Besitzer möchten 100 Prozent Verfügbarkeit, Top-Performance auch in Spitzenzeiten, schnelle Anpassungen und keine unangenehmen Überraschungen. Website Security gehört dabei zu den größten Herausforderungen – denn die Gefahren, die im Internet auf jede einzelne Website lauern, werden nicht nur täglich größer, sondern auch flexibler und komplexer.

Dieses E-Book soll Website-Betreibern und Administratoren helfen, mit möglichst wenig Aufwand ihre Webseiten umfassend abzusichern.

### Sie sind Website-Profi?

Unser E-Book bietet Ihnen Hintergrundwissen und Schritt-für-Schritt-Anleitungen zu Sucuri Website Security.

### Sie sind noch kein Profi, aber interessieren sich für das Thema Website Security?

Eine Erklärung wichtiger Fachbegriffe finden Sie im Glossar am Ende dieses E-Books. Begriffe aus dem Glossar sind im Text **besonders hervorgehoben.**

# Warum auch Sie Ihre Webseite absichern sollten

Stellen Sie sich für einen Augenblick vor, Sie leben für einige Monate im Ausland, und jemand bricht währenddessen in Ihre heimatliche Wohnung ein. Er richtet sich häuslich ein, durchsucht die Schränke, liest Ihre Post und findet vielleicht sogar das Schreiben Ihrer Bank mit dem Telefon-Banking-Passwort. Möglicherweise nutzt er Ihre Adresse für Onlinebestellungen und Ihre Wohnung als Lager für seine Drogengeschäfte – oder er vermietet Ihre Wohnung an andere Gauner. Und Sie bekommen von alldem nichts mit.

Ganz ähnlich verhält es sich, wenn eine Website gehackt wird: Cyber-Kriminelle übernehmen die Kontrolle und nutzen sie für ihre kriminellen Zwecke – häufig ohne dass die Eigentümer der Website etwas davon merken. Täglich passiert das weltweit mehr als 90.000 Mal.[1]

[1] Hosting Facts: Internet Stats & Facts for 2019

## Website-Hacks haben oft gravierende Folgen

Attacken auf Websites nehmen ständig zu (siehe dazu auf der nächsten Seite „Website-Hacks in Zahlen"). Automatisiert und in großem Stil stehlen Hacker Kundendaten und geschäftskritische Informationen, infizieren Website-Besucher mit Malware (bösartiger Software), missbrauchen die Seite für den Versand von Spam-E-Mails, versuchen mit Fremdinhalten und Links Suchmaschinen zu manipulieren oder vermieten Serverleistung und Webspace an andere Kriminelle.

Die Folgen eines erfolgreichen Angriffs sind häufig gravierend: Für viele Unternehmen spielen Websites eine wichtige Rolle für ihre Geschäftsprozesse, etwa in Vertrieb oder Support, als Basis digitaler Services oder im Projektmanagement. Jeder Ausfall kostet Geld und Zeit, stört die Abläufe, beeinträchtigt Reputation und Kundenvertrauen. Zudem können gehackte Websites Hackern ein Einfallstor bieten, um in das Unternehmensnetzwerk einzudringen.

Nicht selten sind gehackte Websites über längere Zeit nicht erreichbar, weil die Hacker Besucher auf andere Websites umleiten oder Suchmaschinen eine als kompromittiert erkannte Seite nicht mehr anzeigen **(Blacklisting). SEO-Spam,** Verunstaltungen **(Defacement)** und Sicherheitswarnungen durch Suchmaschinen können eine Marke nachhaltig beschädigen. Es kann sogar passieren, dass die Cyber-Kriminellen die Website-Datenbank verschlüsseln und dann Lösegeld von den Website-Betreibern verlangen.

## Die Bedrohungslage in Zahlen

- Jede Woche identifiziert der Safe-Browsing-Dienst von Google Tausende manipulierter Websites mit Malware – in der ersten Januarwoche 2019 waren es 3653.[2]
- Im Durchschnitt über 60 Mal täglich wurden 2018 Websites attackiert – die Zahl der Angriffe wuchs von Januar bis Dezember 2018 um knapp 60 Prozent auf 80 pro Tag.[3]
- Fast die Hälfte (44 Prozent) aller Webprofis haben schon erfolgreiche Attacken auf Websites ihrer Kunden erlebt; für Dienstleister mit mehr als 20 Kunden steigt die Wahrscheinlichkeit, einen Hack zu erleben, auf 55 Prozent.[4]
- 13 Prozent aller gravierenden Sicherheitsvorfälle bei KMUs (Kleine und mittlere Unternehmen) sind Folge von Website-Hacking.[5]
- **DDoS-Attacken** auf Webdienste (Distributed Denial of Service) nehmen wieder zu, nutzen mehr Bandbreite und werden länger. Im ersten Quartal 2019 stieg ihre Zahl gegenüber Q4/18 um 84 Prozent an. In Q2/19 verzeichnete Kaspersky einen 509 Stunden (fast 21 Tage) langen DDoS-Angriff.[6]
- Google setzt täglich mehr als 10.000 verdächtige Websites auf seine **Blacklist.** Diese können dadurch bis zu 95 Prozent ihres organischen Traffics verlieren.[7]

---

[2] Google: Transparenzbericht Safe Browsing

[3] SiteLock: 2019 Website Security Report

[4] Sucuri: Web Professionals Security Survey 2019

[5] eco: Studie IT-Sicherheit 2019

[6] Kaspersky: DDoS attacks in Q1 2019 / Q2 2019

[7] Sucuri: How to Remove Google Blacklist Warning

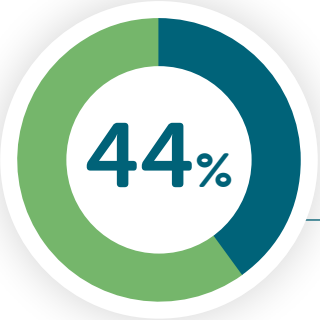
## Website Security: Mythen und Fakten

Noch immer halten sich zum Thema Website Security selbst bei Profis hartnäckig Überzeugungen, die leider längst von der Realität widerlegt wurden. Hier erfahren Sie, warum diese Mythen nicht nur falsch, sondern auch gefährlich sind.

### Mythos 1: Unsere kleine Website ist doch für Hacker uninteressant, bei uns gibt es nichts zu holen.

Das ist leider ein Irrtum. Weil die meisten Angriffe auf Webseiten automatisiert ablaufen, unterscheiden sie nicht nach Website-Größe oder Schadenspotenzial. Bis zu 80 Mal am Tag werden Websites skriptgesteuert angegriffen und auf Schwachstellen getestet – auch die Ihre. Da aber kleine und mittlere Unternehmen in der Regel über weniger Ressourcen und Know-how für die Absicherung ihrer Webpräsenzen verfügen, sind ihre Seiten häufiger anfällig für Malware.

Hinzu kommt: Auch wenn Ihre Website keine Geheimnisse oder Kundendaten bietet, haben Hacker doch garantiert Verwendung für Ihre Domain, Ihren Speicherplatz oder Ihren Webserver – für die Verteilung von Malware oder Spam-Mails, bösartige Umleitungen (Redirects) oder eigene Inhalte für Suchmaschinen (SEO-Spam).

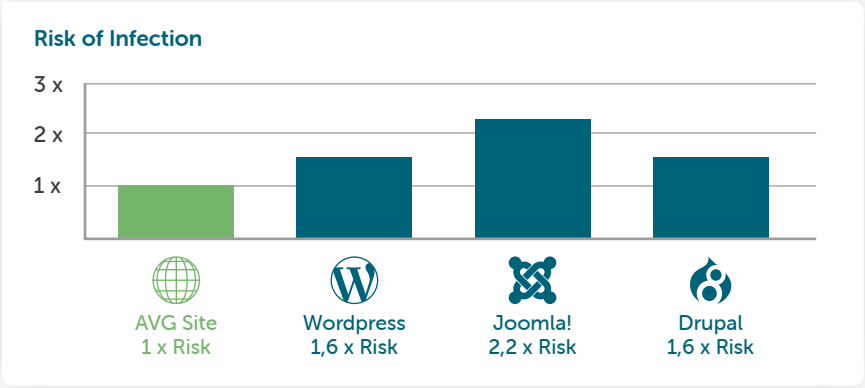



44% aller Web-Professionals müssen mit gehackten Kunden-Webseiten arbeiten.

## Mythos 2: Wir haben ein CMS. Die Security-Profis beim Hersteller sorgen für seine Sicherheit.

Im Gegenteil. Die beliebten Content-Management-Systeme, die vor allem auch von kleinen und mittleren Unternehmen genutzt werden, sind genau deshalb im Visier der Kriminellen. Über die Hälfte (56 Prozent) aller Websites weltweit nutzen ein CMS. Davon ist Wordpress mit einem CMS-Marktanteil von 61 Prozent bei weitem das wichtigste, es wird von knapp 35 Prozent aller Websites genutzt.[8] Entsprechend populär ist dieses CMS bei Hackern: In 2018 ist die Zahl der festgestellten Schwachstellen in WordPress gegenüber 2017 um 30 Prozent auf 542 gestiegen, davon 98 Prozent im Zusammenhang mit Plugins.[9] Ca. 90 Prozent aller mit Malware infizierten CMS-basierten Seiten nutzen WordPress.[10]

Andere CMS sind aber keinesfalls sicherer: Bei Drupal wie WordPress erhöht sich das Risiko einer Infektion um den Faktor 1,6. Bei einer Joomla!-Installation ist es sogar um den Faktor 2.2 höher.[11] Ein besonderes Risiko bei solchen CMS, die in der Regel eine SQL-Datenbank nutzen, besteht in ihrer Anfälligkeit für **SQL-Injektionen**, bei denen über eine Schwachstelle bösartiger Code in die Datenbank eingeschleust und ausgeführt wird.



### Mythos 3: Wir nutzen kein CMS – wir sind also sicher.

Vorsicht: Wahrscheinlich nutzt Ihre Webseite JavaScript. Eine Untersuchung von über 400.000 Websites zeigte, dass 77 Prozent davon mindestens eine Frontend-JavaScript-Bibliothek mit einer bekannten Schwachstelle nutzte (z. B. JQuery).[12] JavaScript kommt zum Beispiel oft in **Cross-Site-Scripting**-Attacken zum Einsatz. Unabhängig von jeder konkret verwendeten Technologie gilt: Es gibt im Web keine absolute Sicherheit!

### Mythos 4: Wir haben lange, komplexe Passwörter und automatische Updates. So haben wir nichts zu befürchten.

Aktuelle Systeme und starke Passwörter sind wichtig, denn sie reduzieren Schwachstellen und erschweren **Brute-Force-Attacken.** Sie bieten aber keinen hundertprozentigen Schutz. Viele Schwachstellen können aus den verschiedensten Gründen nicht automatisch gepatcht werden. Zudem analysieren professionelle Hacker sofort neue Sicherheitspatches ihrer Zielsysteme und starten oft innerhalb weniger Stunden einen angepassten Angriff.

Und auch aktuelle Systeme sind machtlos gegen Angriffe auf Schwachstellen, die noch nicht beseitigt wurden (**Zero-Day-Exploits**). Viele Lücken in Anwendungen oder CMS wie Wordpress und seinen über 50.000 Plugins werden nicht zeitnah geschlossen: Von über 11.000 im ersten Halbjahr 2019 neu gemeldeten Schwachstellen (davon 54 % mit Web-Bezug) wurden 34 Prozent bis Ende August 2019 (also mindestens

[8] W³Techs: Usage of Content Management Systems

[9] Imperva: The State of Web Appliaction Vulnerabilities in 2018

[10] Sucuri: Hacked Website Report 2018

[11] SiteLock: 2019 Website Security Report

[12] Snyk: The State of Open Source Security Report 2017

2 Monate) nicht geschlossen.[13] Wenn Hacker selbst Zero-Day-Exploits entdecken, halten sie diese häufig geheim oder handeln damit im Darknet.

### Mythos 5: Wir sind regelmäßig auf unseren Seiten unterwegs – da fallen uns Unregelmäßigkeiten auf.

Seien Sie sich da nicht so sicher! Es stimmt zwar, dass viele populäre Hacking-Varianten schnell auffallen, zum Beispiel **SEO-Spam** oder Redirects. Die Erfahrung von Sicherheitsdienstleistern zeigt aber, dass sich ein Trend hin zu „stillen" Attacken („Stealth Attacks") ohne für die Websitebetreiber sichtbare Symptome entwickelt, z. B. JavaScript-Dateien, die Besucher infizieren.[14] Das ist eine Reaktion der Cyberkriminellen auf effizientere Security-Abwehrstrategien vor allem auf Seiten der Suchmaschinen (z. B. Google Safe Browsing).

Für einige mögliche Ziele eines Hacks – z. B. Spam-Mail-Versand, Kryptomining, das Stehlen von Informationen oder den Missbrauch des Webservers für eigene Zwecke – ist es zudem unabdingbar, möglichst lange unentdeckt agieren zu können. Das gilt etwa für serverbasierte Attacken (**Backdoors**, **Phishing-Seiten**, bösartige Mailer- oder **DDoS**-Skripts) und auch für website-übergreifende Angriffe wie **XSRF** (**Cross-Site Request Forgery**), bei denen sich der nichtsahnende Nutzer eines kompromittierten Systems bei einer Webanmeldung regulär anmeldet und diese dann attackiert wird.

[13] Riskbased Security: **2019 Mid-Year Vulnerability QuickView Report**

[14] SiteLock: **2019 Website Security Report**

### Mythos 6: Wir nutzen SSL-Verschlüsselung und sind dadurch geschützt.

Die Transportverschlüsselung SSL (Secure Sockets Layer) bzw. heute TLS (Transport Layer Security) ist ein obligatorischer Schutz für Ihre Website und heute auch ein wichtiger Ranking-Faktor. Leider verschlüsselt diese aber nur Datenübertragungen zwischen dem Web-Client Ihres Website-Besuchers und Ihrem Webserver und nicht die Informationen in der Datenbank. Sie erschwert damit zwar Hacker- und Lausch-Angriffe, schützt aber nicht vor Malware, **SQL-Injektion** oder **DDoS-Angriffen**.

## Schlussfolgerungen – Das müssen Sie wissen

1. Jede Website ist täglich Angriffen ausgesetzt.
2. Webseiten mit CMS sind besonders gefährdet.
3. Webseiten brauchen Schutz gegen viele verschiedene Bedrohungen: von Schwachstellen- und Zero-Day-Exploits über Brute-Force- oder Cross-Site-Angriffe bis hin zu DDoS-Attacken.
4. Für umfassende Sicherheit benötigen Websites einen Schutzschild, der zumindest die folgenden Funktionen bieten sollte:
   - Malware-Erkennung und Beseitigung
   - Schutz vor Zero-Day-Exploits
   - Schutz vor Brute-Force-, Injektions- und Cross-Site-Angriffen
   - Schutz vor DDoS-Attacken
   - Sicherheitswarnungen

## Die Konsequenz: Sie benötigen Sucuri Website Security!

Website-Betreiber, die ihre Seiten gegen alle diese Bedrohungen absichern möchten, können die notwendigen regelmäßigen Überprüfungen und Anpassungen manuell durchführen bzw. verschiedene Tools für Malware-Scans, Vulnerability-Scans, Backups etc. nutzen. Besser und mit weniger Aufwand verbunden ist es, auf eine umfassende Website-Security-Lösung zu setzen.

Ein Vergleich der führenden Website Security Suites zeigt, dass Sucuri als einzige die unter Punkt 4 genannten Anforderungen vollständig erfüllt.

### Website Security Suites im Vergleich

| | Sucuri | SiteLock | cWatch | WordFence | OneHour SiteFix |
|---|---|---|---|---|---|
| Malware-Entfernung | unbegrenzt | unbegrenzt | unbegrenzt | Per Cleanup | unbegrenzt |
| Schutz vor Zero-Day-Exploits | ● | | ● | | ● |
| Sicherheits-warnungen | ● | ● | ● | ● | ● |
| Verschlüsselung auch auf dem Firewall Server | ● | | ● | | ● |
| Website Speed- und Performance-Optimierung | ● | ● | ● | | ● |

# Was ist Sucuri Website Security?

Sucuri Website Security ist unsere neue, cloudbasierte Website-Security-Plattform für den umfassenden Schutz Ihrer Websites vor Online-Bedrohungen.

Betrieben wird die Plattform von den erfahrenen Security-Experten von Sucuri (brasilianisch für *Anaconda*), einem weltweit führenden Anbieter von Website-Security-Lösungen und Services. Sucuri ist in über 25 Ländern präsent und wird von Webprofessionals ebenso empfohlen wie von Marktanalysten wie **Gartner.**

## Security-Komplettlösung

Sucuri Website Security kombiniert umfassende und sehr leistungsfähige Security-Funktionen mit einer besonders einfachen Bedienung. Sie ist damit für Einsteiger ebenso geeignet wie für fortgeschrittene Anwender und professionelle Webdienstleister.
Die Plattform schützt Ihre Website vor allen relevanten Security-Bedrohungen im Netz incl. Hackern, Malware, **DDoS-Angriffen** sowie **Blacklisting**. Sie bietet vier Kernfunktionen:

1. Überwachung und Warnung: Intrusion Detection
2. Gefahrenabwehr und Prävention: Firewall
3. Schnelle Reaktion durch Profis: Incident Response Team
4. Schnelle Wiederherstellung im Notfall: Backup & Restore

Die Sucuri-Plattform beinhaltet robuste Website-Überwachung, durchgängigen Schutz und unbeschränkte Bereinigung von Malware- und Blacklist-Einträgen durch Sucuri-Experten. Sie arbeitet reibungslos mit jeder Website-Technologie und jedem CMS  zusammen.

## Mehrwert durch globales CDN

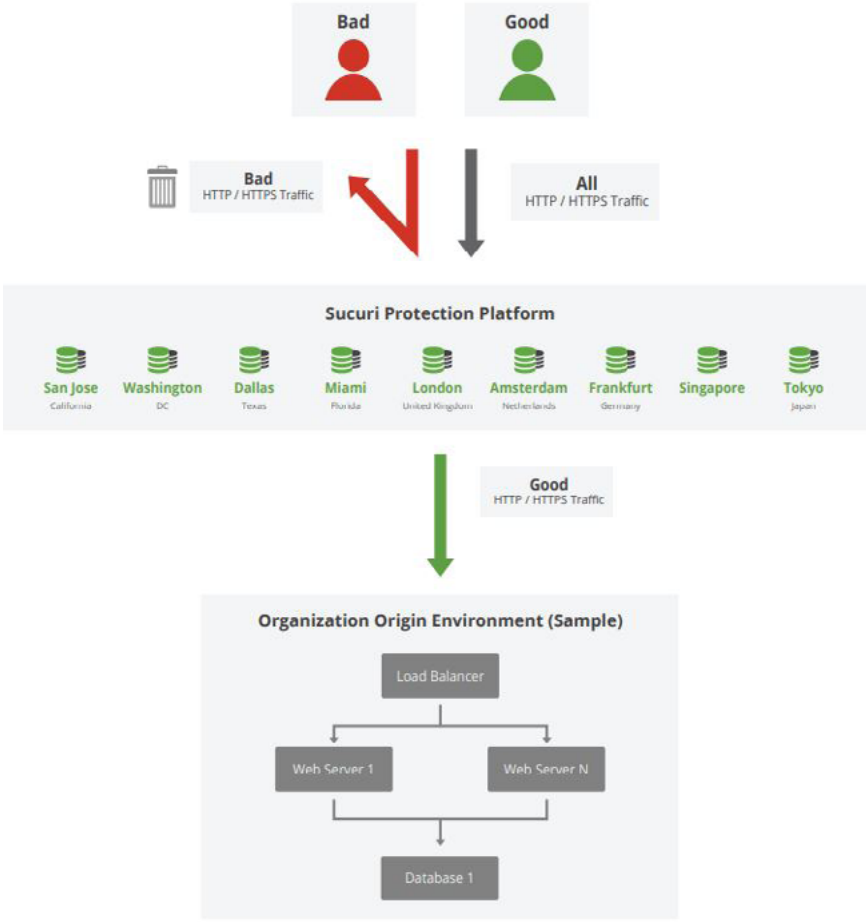
Sucuri Website Security ist eine cloudbasierte SaaS-Lösung (Software as a Service). Sie basiert auf einem weltweiten Netzwerk von Rechenzentren (**Content Delivery Network**, **CDN**), das nicht nur für mehr Sicherheit, sondern auch für optimierte Performance und Verfügbarkeit sorgt.


Quelle: https://sucuri.net/website-performance/

# 10 Gründe, warum Sie Sucuri nutzen sollten

1. Wirksamer Schutz durch Remote-Überwachung
2. Effiziente, nachhaltige Malware-Beseitigung durch Experten
3. Umfassende Prävention: Schutz vor Malware- & DDoS-Angriffen durch cloudbasierte Firewall
4. Höhere Zuverlässigkeit und Verfügbarkeit Ihrer Websites dank CDN
5. Performance-Optimierung für optimale User Experience, Sicherheit und besseres Ranking
6. Schutz Ihrer Online-Sichtbarkeit und Reputation
7. Mehr Transparenz durch umfassende Überwachung, Warnungen und Reports
8. Minimale Betriebsunterbrechung im Schadensfall dank Backup & Restore
9. Vertrauenssiegel auf Ihrer Website: Zeigen Sie Ihren Besuchern, dass Ihre Webseite geschützt ist!
10. Sehr einfach zu administrieren

## Sucuri Website Security:
## Ganzheitlicher Schutz Ihres Netzwerks




Quelle: https://sucuri.net/documentation/Sucuri-Technical-Whitepaper.pdf

# So schützt Sucuri

## Schutzstufe 1: Überwachen und Erkennen

Das Intrusion Detection System von Sucuri scannt regelmäßig alle Ihre Webseiten und erkennt relevante Anzeichen für Kompromittierungen (Indicators of Compromise, IOC). Bei verdächtigen Funden werden Sie umgehend informiert.

### Komplettüberwachung für alle Aspekte Ihrer Website-Security

- **Malware-Scans (Remote)**
  Remote-Überwachung Ihrer Website auf Malware und IOCs – getarnt als Website-Besucher
- **Überwachung von SSL-Zertifikaten**
  Überwachung auf Änderungen am SSL-Zertifikat Ihrer Website
- **SEO-Spam**
  SEO-Spam zuverlässig finden, bevor Google das tut
- **Blacklist-Status**
  Überwachung auf Security-Warnungen von Blacklist-Anbietern
- **Website-Verfügbarkeit**
  Bei Ausfällen sofort aktiv werden können
- **DNS-Überwachung**
  Alarmierung bei Veränderungen an Ihren DNS-Einstellungen

### Verdacht auf Kompromittierung? Unsere Experten reagieren schnell und professionell.

Wenn Sie eine Warnmeldung erhalten oder verdächtige Aktivitäten registrieren, können Sie jederzeit ein Cleanup beantragen. Wir sorgen für eine nachhaltige Bereinigung Ihrer Website.

## So einfach aktivieren Sie die Überwachung (alle Pakete)

1. Melden Sie sich in Ihrem Sucuri Dashboard an und klicken Sie auf **„Website Monitoring“**.
2. Klicken Sie **„Add Site“** und geben Sie die URLs Ihrer Websites ein. Der Remote Scanner ist sofort aktiviert und beginnt mit der Analyse.
3. Weitere Überwachungen (Blacklist-Status, DNS, SSL, Uptime) und Überwachungsfrequenzen konfigurieren Sie unter **„Settings“ – „Monitoring Types“**.
4. Warnmeldungen per E-Mail sind im Standard aktiviert. Andere Optionen (SMS, Slack, RSS, Custom Posts) sowie wöchentliche/monatliche E-Mail-Reports können Sie in Ihren globalen Profil-einstellungen konfigurieren.

Mehr Infos: https://sucuri.net/guides/getting-started-with-sucuri/

## Schutzstufe 2: Abwehr von Hacks und Angriffen

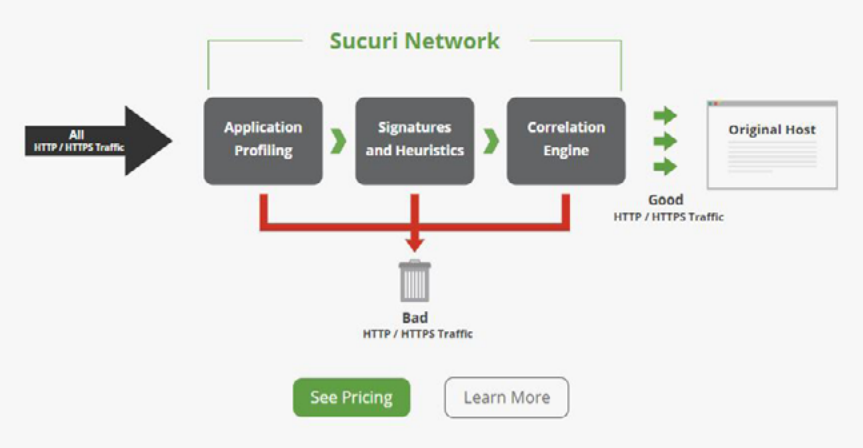
Die Sucuri Firewall schützt Ihre Website in Echtzeit vor Bedrohungen und steigert gleichzeitig ihre Performance. Sie kombiniert eine **Website Application Firewall (WAF)** für Schutz auf Anwendungsebene mit einem **Intrusion Prevention System (IPS)** für Website-Schutz auf Netzwerkebene. Die Sucuri Firewall basiert auf unserem leistungsfähigen **Content Delivery Network (CDN)** und Machine-Learning-Technologie. So kann sie den für Ihre Website bestimmten Netzwerkverkehr von bösartigen Anfragen befreien, noch bevor sie Ihren Server erreichen. Durch **Virtual Patching** und **Virtual Hardening** reduziert die Sucuri-Firewall die Angriffsfläche ihrer Website für Attacken.

### Sucuri Firewall hält Gefahren von Ihrer Website fern

- **Schutz vor Malware und Hackern**
  Abwehr automatisierter und manueller Angriffe
- **Schutz vor Zero-Day-Exploits**
  Abschirmung ungepatchter Schwachstellen durch Blockade verdächtiger Aktivitäten
- **Schutz vor DDoS-Attacken**
  Zuverlässige Blockade von Attacken auf Netzwerk- und Anwendungsebene
- **Schutz vor Brute Force-Attacken**
  Abwehr von automatisierten Passwort-Cracking-Versuchen

## Verschiedene Schutzschichten

- Virtual Patching & Hardening
- Besonderer Schutz kritischer Seiten
- Anwendungsprofile
- Angriffsmuster und Signaturen
- Blockade bösartiger Bots
- Geoblocking (Als Betreiber eines Online-Shops sollten Sie die EU-Geoblocking-Verordnung beachten!)




Quelle: https://sucuri.net/website-firewall/

Die Sucuri Firewall erfordert keine Installation von Software oder Änderungen an Ihren Anwendungen. Sie aktivieren den Schutz Ihrer Website über Ihre DNS-Einstellungen.*

Die Sucuri Firewall ist in den Sucur-Paketen Deluxe und Ultimate enthalten.

* Sucuri Firewall schützt als Proxy den Netzwerkverkehr über Port 80 (HTTP) und 443 (HTTPS). Falls Ihre Anwendung an einem anderen Port läuft, nutzen Sie bitte eine Subdomain, die direkt auf Ihre Hosting-IP zeigt, oder einen Reverse Proxy auf Port 80 oder 43.

## So aktivieren Sie die  Sucuri Firewall (Deluxe, Ultimate)

1. Melden Sie sich im Kunden-Informations-System von Host Europe (KIS) an und gehen Sie zu **„Produktverwaltung“** – **„Website Security“**.
2. Melden Sie sich über den Button **„Jetzt starten“** in Ihrem Sucuri Dashboard an und klicken Sie auf **„Verwalten“** neben dem gewünschten Paket. Danach gehen Sie zum Menüpunkt **„Firewall“**.
3. Nun müssen Sie die DNS-Einträge einrichten. Dafür werden Ihnen mehrere Möglichkeiten Angeboten.
4. Klicken Sie nach der DNS-Einrichtung auf **„Firewall aktivieren“**. Die Sucuri Firewall beginnt nun mit dem Speichern Ihrer Website in ihrem Puffer-Cache.
5. Testen Sie mithilfe der internen Domain, ob das Caching erfolgreich war, indem Sie auf den Link unter **„Einstellungen“** – **„Interne Domains“** klicken. Bei Fehlermeldungen versuchen Sie es nach einigen Minuten erneut. HTTPS müssen Sie während des Tests temporär deaktivieren.
6. Whitelisten Sie gegebenfalls die Firewall-IP in Ihrer Server-Firewall. Laden Sie Ihr eigenes SSL-Zertifikat hoch und/oder schützen Ihren Server vor dem Direktzugriff mittels Server-IP.

## Schutzstufe 3: Website-Backups und Wiederherstellung (nur verfügbar bei Sucuri Ultimate)

Egal, was Sie tun, um Ihre Website abzusichern – das Risiko wird nie gleich Null sein. Im Notfall stellt der Backup-Service von Sucuri den kontinuierlichen Betrieb Ihrer Website sicher.

Im Gegensatz zu gängigen Plugin-Backuplösungen speichert Sucuri alle Dateien und Datenbanken Ihrer Websites sicher und zuverlässig auf externen Servern in seinem Netzwerk. Tritt ein Problem mit Ihrer Installation auf – zum Beispiel durch Hardwaredefekt, Softwarefehler, Malwarebefall oder Fehlkonfiguration –, können Sie mit wenigen Mausklicks einen früheren Zustand Ihrer Wahl wiederherstellen.

### Disaster Recovery für Ihre Website

- **Externe Backups**
  Sichere Speicherung von Dateien und Datenbanken außerhalb Ihrer Hosting-Infrastruktur
- **Einfach, schnell und sicher**
  Start, Konfiguration und Wiederherstellung/Download über das Sucuri Dashboard
- **Flexible Zeitpläne und Benachrichtigungen**
  Automatisches Backup (täglich, wöchentlich, monatlich), optionale Benachrichtigungen und Fehlerwarnungen
- **Sichere Speicherung**
  Hochsichere Sucuri-Infrastruktur lässt Hackern keine Chance
- **Backups für 90 Tage**
  Exakte und komplette Wiederherstellung Ihrer Website in der Version eines beliebigen Tags der letzten drei Monate

## Profi-Funktionen für Ihre Sicherheit

- Flexibel konfigurierbar
- Unabhängig von Webhost oder CMS
- Dateisystem-Backup über FTP/SFTP
- Volles erstes Backup und inkrementelle Speicherung geänderter Dateien
- Automatische Erkennung von MySQL-Datenbanken
- Ausgewählte Verzeichnisse können vom Backup ausgenommen werden
- Einfache und schnelle Wiederherstellung nach Tag
- Download oder automatische Wiederherstellung von Backups über das Sucuri Dashboard
- Support verfügbar


Quelle: https://sucuri.net/website-backups/

Der Backup-Service funktioniert mit jeder Hosting-Technologie und auf jedem CMS. Sie benötigen lediglich ein FTP- bzw. SFTP-Zugang zu Ihrem Hosting-Produkt. Es ist keine Installation von Software erforderlich oder Änderungen an Ihren Anwendungen. Sie können Ihre Websites über das Sucuri Dashboard hinzufügen und konfigurieren. Backups sind **nur im Paket Sucuri Ultimate** enthalten.

## So einfach aktivieren Sie Backups für Ihre Websites (Ultimate)

1. Melden Sie sich im KIS von Host Europe an und gehen Sie zu **„Produktverwaltung“** – **„Website Security“**.
2. Melden Sie sich über den Button **„Jetzt starten“** in Ihrem Sucuri Dashboard an und klicken auf **„Verwalten“** neben dem gewünschten Paket. Danach gehen Sie zum Menüpunkt **„Backups“**.
3. Klicken Sie auf **„Einstellungen“** und geben Sie Ihre (S)FTP-Zugangsdaten ein und klicken Sie **„Speichern“**.
4. Wählen Sie die Datenbank-Einstellungen aus und klicken Sie **„Speichern“**. Das System kann automatisch MySQL-Datenbanken erkennen.
5. Konfigurieren Sie die Backup-Frequenz, die Startzeit und legen Sie fest, ob bzw. wann Sie benachrichtigt werden möchten. Ihre Backups starten automatisch.

## Wiederherstellung von Dateien und Datenbanken

1. Melden Sie sich in Ihrem Sucuri Dashboard an und klicken Sie auf den Reiter „**Backups**“.
2. Wählen Sie das wiederherzustellende Backup aus und klicken Sie „**Restore Options**“.

   **Dateien:** Sie können alle oder einzelne Dateien herunterladen, per E-Mail versenden oder aber automatisch wiederherstellen.

   **Datenbank:** Sie können Datenbank-Backups downloaden oder automatisch wiederherstellen.

## Im Schadensfall: Nachhaltige Säuberung durch Experten

Eine schnelle und nachhaltige Schadensbehebung stellt sicher, dass Security-Vorfälle nicht Ihr Geschäft und Ihre Reputation beschädigen. Mit dem engagierten Security Incident Response Team (SIRT) von Sucuri sind Sie auf der sicheren Seite.

### Das tun wir für Sie im Schadensfall

- **Malware-Bereinigung und komplette Wiederherstellung**
  Entfernung bösartigen Codes aus Dateisystem und Datenbank
- **Löschen von Blacklist-Einträgen**
  Übermittlung von Blacklist Removal Requests für Ihre Seiten
- **Reparieren von SEO-Spam**
  Entfernung von SEO-Spam-Keywords und Links

## Auch komplexe Infektionen schnell und sicher beseitigen

Security-Vorfälle und Bedrohungen können viele Gesichter haben, und automatisierte Verfahren zu Schadensbehebung sind oft nicht nachhaltig erfolgreich. Unser SIRT analysiert sorgfältig jeden Einzelfall und spürt auch versteckte Malware, installierte **Backdoors** und Mehrfachbefall auf.

## Automatische und manuelle Bereinigung

Wir nutzen Skripte und Werkzeuge, um Ihre Website schnell auf Malware zu durchsuchen. Zudem überprüfen unsere Analysten Ihre Website von Hand. Kein Hack ist zu komplex für unsere erfahrenen Security-Profis, die Zugriff auf unsere ausgefeilte **Threat Intelligence** haben und auch aktuelle Malware-Kampagnen im Auge behalten.

## Ihre Vorteile

- Nachhaltige Schadensbehebung
- Schnelle Reaktionszeiten
- Unbeschränkte Cleanups
- Zuverlässiger Support

## Sie behalten die Kontrolle

Zur Beseitigung von Malware müssen wir Veränderungen an Ihrer Website vornehmen. Mit Ihrem Auftrag erklären Sie uns dafür Ihr Einverständnis. Grundsätzlich werden von uns keine Passwörter gespeichert. Passwörter werden ausschließlich für die automatische Bereinigung selbst genutzt und anschließend gelöscht.

## So fordern Sie eine Malware-Bereinigung für Ihre Website an

1. Melden Sie sich im KIS von Host Europe an und gehen Sie zu **„Produktverwaltung“** – **„Website Security“**.
2. Melden Sie sich über den Button **„Jetzt starten“** in Ihrem Sucuri Dashboard an und klicken auf **„Verwalten“** neben dem gewünschten Paket. Danach gehen Sie zum Menüpunkt **„Säubern“**.
3. Klicken Sie **„Neue Malware Removal Request“**.
4. Geben Sie die betroffene Website, die Problemkategorie sowie Ihre Verbindungs- und Zugangsdaten ein und klicken Sie **„Anfrage einreichen“**. Falls das System nicht auf Ihre Website zugreifen kann, erhalten Sie eine Warnmeldung. Sie können dann die Zugangsdaten korrigieren oder auf **„Anfrage trotzdem einreichen“** klicken.

# 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