Whitepaper

Sucuri Website Security für Onlineshops

Tipps für Agenturen und Betreiber von Webshops und anderen traffic-starken Websites

Powered by Sucuri

Domain Factory

Inhaltsverzeichnis

Sicherheit und Verfügbarkeit für Webshops 3
- Ihr Nutzen 4

Onlineshops brauchen besonderen Schutz 5
- Automatisierte Attacken nehmen zu 5
- Hohes Schadenspotenzial 8
- Gezielte Angriffe auf High-Traffic-Sites und Shops 9
- DDoS-Attacken legen Webshops lahm 10
- WordPress-Shops sind besonders gefährdet 11
- Veraltete Systeme haben Sicherheitslücken 12

Herausforderungen für Shop-Betreiber und Dienstleister 13
- Verfügbarkeit gewährleisten: Rundum-Schutz erforderlich 13
- Sicherheit erfordert Zeit und Aufwand 13
- Schnelle Problemlösung bei Malware-Befall? 15
- Sicherheit und Verfügbarkeit – einfach und kostengünstig 15

Szenarien 16
- Praxisbeispiel 1: Ransomware-Infektion 16
- Praxisbeispiel 2: Verfügbarkeit am Black Friday sichern 19

Sucuri-Sicherheitsfunktionen 21
- Überwachung: Erkennung von Malware und Blacklisting 21
- Schnelle Reaktion: Professionelle Malware-Bereinigung 21
- Sucuri Firewall: Prävention in Echtzeit 22
- Content Delivery Network: Optimierte Verfügbarkeit und Performance 22
- Backups: Sicherung und Wiederherstellung im Notfall 23

Sucuri Website Security: Tarifoptionen 23
- Passende Pakete für unterschiedliche Anforderungen 23
- Alle Sucuri-Pakete auf einen Blick 25

Management Summary

Sicherheit und Verfügbarkeit für Webshops

Für Sie als Betreiber eines Webshops, einer Onlineplattform oder einer anderen traffic-starken Onlinepräsenz ist Ihre Website wahrscheinlich die wichtigste Einnahmequelle. Sie haben viel investiert, um dahin zu gelangen, wo Sie jetzt stehen – in SEO, guten Content und performantes Hosting. Denn Sichtbarkeit und Verfügbarkeit Ihrer Website sind für Sie erfolgskritisch – jeder Ausfall („Downtime“) kostet viel Geld und beeinträchtigt zudem Image und Kundenvertrauen.

Aber Websites sind heute mehr denn je bedroht durch Angriffe aus dem Netz: automatisierte Bot-Attacken, Malware-Infektionen und Hacks, aber auch Brute-Force- oder DDoS-Angriffe. Nicht nur die Anzahl von Hacker-Attacken steigt ständig, sie werden auch immer komplexer, ausgefeilter und effizienter. Gerade Webshops sind dabei für Hacker besonders interessant: Denn das Erpressungspotenzial ist hier viel größer als bei Standardwebsites oder Blogs und außerdem können hier wertvolle Kundendaten abgegriffen werden, zum Beispiel Kreditkartendaten.

Deshalb müssen Sie als Onlineshop-Betreiber oder Webdienstleister diese Webseiten besonders sorgfältig schützen. Sie müssen dafür die nötigen Security-Kompetenzen aufbauen und zudem ausreichend Ressourcen vorhalten, denn die Absicherung von Websites erfordert viel Zeit und ständige Aufmerksamkeit. Wenn dann allerdings nicht genug Budget für Website-Security vorhanden ist, stehen Sie vor einem gravierenden Problem.

Die Lösung heißt Sucuri Website Security. Die kostengünstige cloudbasierte Security-Suite von Sucuri überwacht Ihre Websites auf alle relevanten Anzeichen einer Kompromittierung: Malwarebefall, SEO-Spam, Unregelmäßigkeiten bei SSL- oder DNS-Einstellungen, Verfügbarkeitsprobleme oder Blacklisting-Ereignisse. Wird Sucuri fündig, sorgen erfahrene Malware-Experten für eine schnelle und vollständige Bereinigung. Auf Wunsch schützen die CDN-basierte Sucuri Firewall, sichere Backups und globales Caching Ihre Websites in Echtzeit vor Cyber-Bedrohungen und gewährleisten jederzeit eine hohe Verfügbarkeit.

Ihr Nutzen

Umfassender Schutz

Sucuri schützt Ihren Online-Shop gegen alle Bedrohungen aus dem Netz.

Maximale Verfügbarkeit

Permanente Überwachung und Caching auf performanten Sucuri-Servern weltweit schützt Ihre Website zuverlässig vor Ausfällen oder Überlastung.

Soforthilfe im Schadensfall

Bei Hacks und Malware-Befall sorgt Sucuri für eine schnelle und gründliche Problemlösung: dank jederzeit aktueller Backups und kompetenter Malware-Bereinigung durch Experten.

Aufwand und Kosten sparen

Sucuri Website Security schützt Webshops und Online-Plattformen deutlich kostengünstiger als vergleichbare Services.

Onlineshops brauchen besonderen Schutz

Weil Sie als Shop-Betreiber stabile Umsätze brauchen, müssen Sie proaktiv für die Sicherheit Ihrer Website sorgen – im eigenen Interesse und im Interesse Ihrer Kunden, für deren sensible Daten Sie verantwortlich sind. Stellen Sie sich vor, als Onlinekäufer finden Sie heraus, dass Hacker bei einem von Ihnen genutzten Webshop Ihre Zahlungsinformationen erbeutet haben. Bei diesem Shop werden Sie wahrscheinlich nicht mehr einkaufen.

Vertrauen spielt im E-Commerce eine wichtige Rolle. Wenn Ihr Onlineshop nicht vertrauenswürdig und sicher erscheint, werden sich Ihre Kunden woanders umsehen. Wird Ihr Shop gehackt oder mit Malware infiziert, leiden nicht nur Kundenvertrauen und Ihr gutes Image, sondern auch Ihre Umsätze. Denn während Sie versuchen, Ihre Website zu bereinigen, verpassen Sie Stunde für Stunde potenzielle Verkäufe.

Automatisierte Attacken nehmen zu

Attacken auf Websites nehmen seit Jahren zu. Mehr als 90.000 Websites werden täglich gehackt (Quelle: Hosting Facts Internet Stats & Facts for 2019). Ein großer Teil dieser Angriffsziele gehört zu Onlineshops.

Ein Grund für die steigende Gefahr: Immer mehr Angriffe laufen automatisiert ab. Durchschnittlich 60 Mal am Tag bekommt eine Website Besuch von sogenannten Bad Bots (Quelle: Sitelock Security Report 2019). Auch E-Commerce-Sites werden immer häufiger und auch zunehmend raffinierter von Bots attackiert. Kriminelle versuchen auf diese Weise, Kundenkonten zu übernehmen, Geschenkkarten zu missbrauchen, Spam-Kommentare zu hinterlassen oder Transaktionsbetrug zu begehen. Andere Bad Bots scannen beispielsweise im Auftrag von Konkurrenten Angebote und Preise, sammeln Finanzinfos für Investmentgesellschaften oder kaufen

in Massen begehrte Waren auf, damit Reseller sie teuer weiterverkaufen können (sogenannte Sneaker Bots oder Grinch Bots). Solche Aktivitäten beeinträchtigen nicht nur Kundenerlebnis und Marke, sondern können auch Performance-Einbrüche und sogar Ausfallzeiten zur Folge haben (Quelle: Imperva, „How Bots Affect E-commerce“, 2019).

Sucuri Firewall blockiert Millionen Bot-Angriffe

2019 blockierte die Firewall von Sucuri knapp 27 Millionen Bad-Bot-Angriffe. Damit nahmen Bad Bots unter allen verzeichneten Angriffsarten Platz 1 ein (Abbildung 1). Insgesamt blockierte die Sucuri Firewall fast 171 Millionen Angriffsversuche – 52 Prozent mehr als 2018 (Quelle: Sucuri Website Threat Research Report 2019).

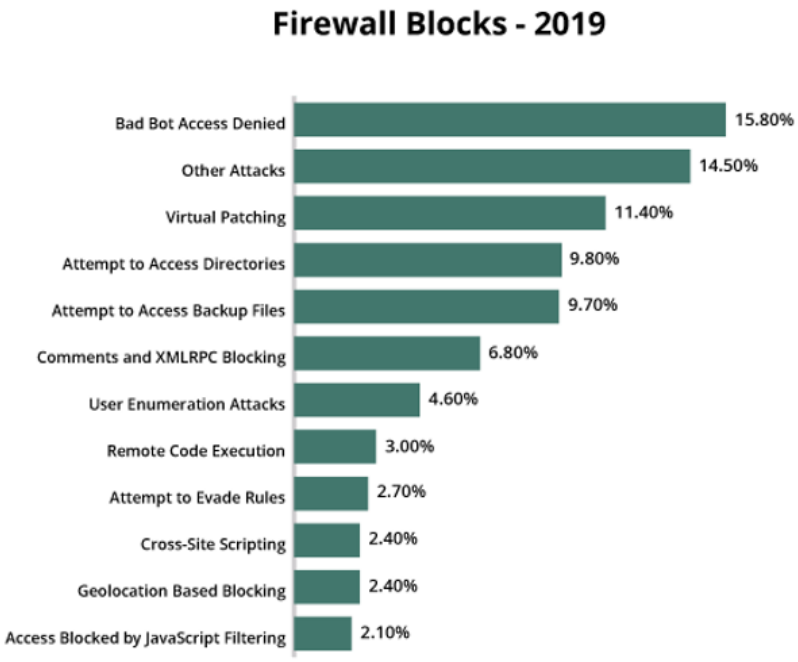

Abbildung 1: Die Sucuri Firewall blockierte 2019 fast 171 Millionen Angriffsversuche (Quelle: Sucuri).

Hohes Schadenspotenzial

Ist die Schwachstellensuche oder ein Brute-Force-Angriff auf die Login-Seite erfolgreich, folgen meist automatisch gezielte Aktionen: Die Angreifer versuchen Dateistruktur und Datenbank zu erkunden, Malware zu installieren, die Website zu entstellen oder SEO-Spam einzuschleusen. Der Schaden für die Website-Betreiber reicht von Datendiebstahl und Kontrollübernahme über Betriebsstörungen und Downtimes bis hin zu Erpressung mit hohen Lösegeldforderungen.

Zudem ist mit Folgeschäden zu rechnen, zum Beispiel durch das sogenannte Blacklisting. Google oder auch große Web-Security-Unternehmen wie McAfee führen Listen mit Websites, bei denen sie Anzeichen von Malware oder anderen Sicherheitsbedrohungen finden. Halten Suchmaschinen Ihre Webseite für gefährlich, weil diese auf einer dieser Listen steht, zeigen die Suchmaschinen diese nicht mehr in ihren Suchergebnissen an oder geben eine Sicherheitswarnung aus („Diese Website kann Ihren Computer beschädigen“). Wöchentlich identifiziert Googles Safe-Browsing-Dienst ca. 30.000 Websites als potenziell schädlich.

Ist Ihre Website von Blacklisting betroffen, schädigt das Ihr Image und es kostet zudem viel Zeit und Aufwand, um die Seite wieder von der Blacklist zu entfernen.

Gezielte Angriffe auf High-Traffic-Sites und Shops

Während Angriffe auf E-Commerce-Sites, insbesondere zum Zweck des Kreditkartendiebstahls, früher eher wahllos eine große Zahl von Websites ins Visier nahmen, geht der Trend neuerdings hin zu gezielteren Angriffen auf populäre Seiten mit viel Traffic und größerer Nutzerbasis – oder auf entsprechend populäre Systeme wie WordPress oder Magento (Quelle: Sucuri Website Threat Research Report 2019).

Prominentes Beispiel sind sogenannte Magecart-Angriffe. Magecart ist ein wahrscheinlich schon seit 2010 aktives Syndikat krimineller Hackergruppen, die sich darauf spezialisiert haben, Kundendaten und Zahlungsinformationen von Online-Shopping-Cart-Systemen, vor allem Magento, zu stehlen. Sie und ihre Nachahmer versuchen beispielsweise, Schadcode direkt in Warenkorb- und Checkout-Prozesse einzuschleusen, um die gewünschten Daten abzuschöpfen („Skimming“). Dabei greifen sie bevorzugt Hilfsressourcen an, die von den Shopsystemen genutzt werden, von der Webserver-Datenbank bis hin zu Cloud-Ressourcen, zum Beispiel schlecht konfigurierte Amazon-S3-Webservices.

Mehr als 18.000 Websites waren bis Oktober 2019 von Magecart-Angriffen betroffen, darunter Ticketmaster und British Airways, so ein Bericht der Analysefirma RiskIQ. Ende 2019 wurde dann bekannt, dass Angreifer inzwischen sogar einen Anbieter schlüsselfertiger E-Shops mit mehr als 20.000 Kunden geknackt haben: Im Oktober hat der E-Commerce-Cloudanbieter Volusion unwillentlich Magecart-Schadcode an mindestens 6.500 Webshops ausgeliefert. Viele Experten sind sich sicher, dass solche und ähnliche Angriffe weiter zunehmen werden

Hacker gehackt

Übrigens sind auch kriminelle Shops im Dark Web nicht vor Hackerangriffen gefeit: Im Sommer 2019 wurde „BriansClub“, einer der größten Online-Schwarzmärkte für gestohlene Kreditkartendaten, gehackt und eine Datenbank mit 26 Millionen Kredit- und Debitkarten-Datensätzen kopiert. Der Inhalt entspricht einem Schwarzmarktwert von über 400 Millionen Dollar.

DDoS-Attacken legen Webshops lahm

Im Dark Web können Kriminelle nicht nur gestohlene Account- oder Kartendaten kaufen. Für wenig Geld (beginnend bei unter 5 Dollar) kann dort praktisch jeder einen massiven Überlastungsangriff (Distributed Denial of Service, DDoS) auf die Website seiner Wahl durchführen lassen – zum Beispiel auch Ihr Konkurrent oder ein unzufriedener Kunde. Möglich machen das DDoS-as-a-Service-Provider, sogenannte Booter-Dienste. So finden einer aktuellen Untersuchung zufolge am weltweit größten Internetknoten DE-CIX in Frankfurt rund um die Uhr DDoS-Angriffe gegen Tausende Ziele im Internet statt. Während die maximalen Angriffslasten noch vor kurzem unter 600 Gbps (Gigabit per Sekunde) lagen, sind sie inzwischen im Terabit/s-Bereich angekommen. Wie sich zeigte, hilft es auch wenig, solche Booter-Webseiten vom Netz zu nehmen, weil das die eigentliche DDoS-Infrastruktur (gekaperte Computer, IoT-Geräte etc.) kaum beeinträchtigt.

DDoS-Angriffe werden mit dem Ziel gestartet, Schaden anzurichten oder aber das Opfer zu erpressen. Sie verursachen meist erhebliche Performance-Einbrüche bis hin zu Komplettausfällen, die Stunden andauern können. Für Webshops sind solche Attacken besonders bedrohlich, da sie meist direkte Umsatzeinbußen zur Folge haben.

Saisongeschäft für Cyber-Kriminelle

Das gilt natürlich vor allem für Spitzenzeiten wie das Weihnachtsgeschäft, Black Friday oder Cyber Monday – und genau dann steigt die Zahl der DDoS-Angriffe auf E-Commerce-Seiten um über 70 Prozent (Quelle: BSI-Bericht „Die Lage der IT-Sicherheit in Deutschland 2019“).

WordPress-Shops sind besonders gefährdet

Viele Webshops nutzen als Basis das Content-Management-System WordPress. Die weltweit meistgenutzte E-Commerce-Plattform ist ein WordPress-Plugin – WooCommerce mit einem Anteil von knapp 30 Prozent (in Bezug auf Installationen; Quelle: Datanyze.com). Seine Popularität macht WordPress zu einem beliebten Ziel für Hacker- und Malware-Attacken. Sie versuchen, sich die Tausenden von Schwachstellen in WordPress-Core, Plugins und Themes zu Nutze zu machen. Vor allem Plugins sind gefährdet, Shop-Plugins ebenso wie viele andere.

Zum Beispiel machten 2019 wieder zahlreiche Schwachstellen in WooCommerce selbst oder seinen Erweiterungen Schlagzeilen. Kritisch in diesem Zusammenhang sind auch kommerzielle Plugins, weil diese häufig nicht im WordPress-Repository liegen und daher weniger regelmäßig aktualisiert werden. Das betraf etwa eine Ende Februar 2020 gepatchte Sicherheitslücke im Plugin WooCommerce Smart Coupons, bei dem sich Angreifer gültige Gutscheine selbst generieren konnten. Ebenfalls im Februar 2020 wurde eine Zero-Day-Lücke im Plugin Flexible Checkout Fields for WooCommerce geschlossen, die bereits eine Zeit lang unerkannt für Hacks ausgenutzt worden war.

Veraltete Systeme haben Sicherheitslücken

Eine wichtige Ursache für Sicherheitsprobleme sind veraltete Systeme. Für Webshops gilt das in besonderem Maße. Bei WordPress-basierten Systemen erschwert der Einsatz kommerzieller Plugins das regelmäßige Aktualisieren, bei Magento die verschiedenen Entwicklungszweige. 49 Prozent aller WordPress-Sites sowie 87 Prozent der Magento-Websites, bei denen Sucuri einen Malware-Befall festgestellt hat, waren zum Zeitpunkt der Infektion veraltet (Quelle: Sucuri Website Threat Research Report 2019).

Zudem wird Magento ab Juni 2020 keine Software-Updates und Sicherheits-Patches für seine beliebten Commerce 1- und Open-Source-CMS-Plattformen (ehemals Enterprise- und Community-Editionen) mehr bereitstellen. Wer nicht zeitnah auf eine noch unterstützte Plattform migrieren kann, sollte zum Schutz unbedingt eine zuverlässige Website-Firewall mit Virtual Patching nutzen, wie sie Sucuri bietet.

Herausforderungen für Shop-Betreiber und Dienstleister

Verfügbarkeit gewährleisten: Rundum-Schutz erforderlich

Aus diesen Gründen benötigen Onlineshops und -plattformen besonderen Schutz – denn von ihrer uneingeschränkten Verfügbarkeit hängt die wirtschaftliche Existenz ihrer Betreiber ab.

Neben den üblichen Sicherheitsmaßnahmen zum Schutz vor Malware und Hacks ist dabei vor allem auch der Schutz vor Überlastung wichtig, sei es – im positiven Fall – durch einen Kundenansturm am Black Friday oder durch den DDoS-Angriff eines Erpressers oder Konkurrenten.

Sicherheit erfordert Zeit und Aufwand

Sicherheitsmaßnahmen sind aber aufwendig – regelmäßige Updates reichen da nicht aus. Eine große Gefahr, gegen die es keine Sicherheitspatches gibt, sind Brute-Force-Angriffe: Dabei probieren Hacker automatisiert viele Tausend oder Millionen Login-Kombinationen aus, häufig auf Basis gestohlener Datenbanken mit echten Zugangsdaten. Kritisch sind auch Angriffe auf Schwachstellen, die noch nicht geschlossen wurden, entweder weil sie den Entwicklern noch gar nicht bekannt sind (Zero-Day-Exploits) oder weil die Entwickler noch keinen Patch liefern konnten.

Bei der Absicherung von Websites muss vor allem der Schutz gegen die Angriffsmethoden SQL Injection (SQLI), Remote/Local File Inclusion (RFI/LFI) und Cross-Site Scripting (XSS) gewährleistet werden. Injection-Attacken machen dabei laut Akamai über 65 Prozent der Angriffe auf Webanwendungen aus (siehe Abbildung 2); sie liegen auch bei den OWASP Top Ten an der Spitze.

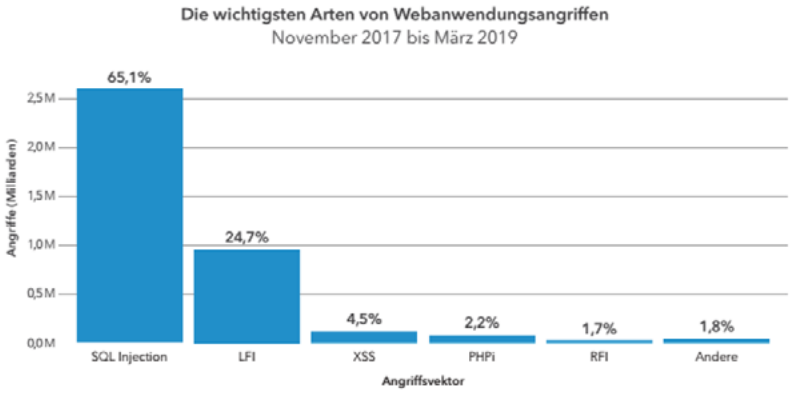

Abbildung 2: SQL Injection war 2019 die wichtigste Angriffsart.

Alle diese Angriffe nutzen Schwachstellen aus, die auf der unsicheren Behandlung von Nutzereingaben beruhen. Um sie abzuwehren, können Sie etwa Formulare etc. durch Captchas schützen, User-Input validieren und bereinigen sowie auch Datenausgaben bereinigen und maskieren.

Darüber hinaus müssen Websites regelmäßig auf Schwachstellen und Anzeichen für Kompromittierungen überprüft werden. Auch regelmäßige Backups sind natürlich wichtig. Allerdings fehlt vielen Webmastern oder Dienstleistern die Zeit oder zum Teil auch das Wissen, um alle diese Maßnahmen selbst durchzuführen.

WordPress-Anwender könnten ein Security-Plugin nutzen, das ihnen einige dieser Aufgaben abnimmt. Aber auch das ist nicht unproblematisch, weil auch Security-Plugins Sicherheitslücken aufweisen können.

Schnelle Problemlösung bei Malware-Befall?

Reiner Schutz ist aber ebenfalls nicht genug: Weil es im Internet keine 100-prozentige Sicherheit geben kann, brauchen Sie als Shop-Betreiber oder Betreuer auch einen Plan B, wenn es trotzdem zu einem Malware-Befall kommt.

Cyberangriffe werden nicht nur immer häufiger, sondern auch komplexer. Moderne Malware versteckt sich heute meist an vielen Stellen einer Website und versucht auch andere Websites auf dem gleichen Server zu infizieren. Sie verfügt oft über Selbstheilungsmechanismen, um sich bei einer unvollständigen Säuberung erneut zu installieren, und richtet sehr häufig auch Backdoors für einen unbemerkten späteren Zugriff ein. Von über 60.000 infizierten Websites, die Sucuris Malware-Profis 2019 bereinigt haben, fanden sich auf fast der Hälfte eine oder mehrere Backdoors (Quelle: Sucuri Website Threat Research Report 2019).

Für die Bereinigung ist ein sauberes und halbwegs aktuelles Backup hilfreich, aber auch Backups können bereits infiziert sein, wenn ein Angriff erst nach einiger Zeit bemerkt wurde. Es kann daher unter Umständen schwer oder unmöglich sein, den aktuellen Zustand zu rekonstruieren.

In jedem Fall erfordert die manuelle Bereinigung einer mit Malware infizierten Website viel Zeitaufwand und auch viel Know-how. In der Regel benötigen auch Webprofis Tage, um eine kompromittierte Seite komplett wiederherzustellen – in dieser Zeit kann Ihnen sehr viel Umsatz verloren gehen.

Sicherheit und Verfügbarkeit – einfach und kostengünstig

Für all diese Herausforderungen ist Sucuri Website Security die einfachste und kostengünstigste Lösung. Sucuri bietet Ihnen nicht nur Rundum-Schutz für Ihre Website (mit Malware-Scans, Web Application Firewall,

Whitelisting/Blacklisting-Funktionen oder Backups), sondern auch professionelle Malware-Bereinigung im Schadensfall sowie maximale Verfügbarkeit dank Content Delivery Network (CDN).

Szenarien

Praxisbeispiel 1: Ransomware-Infektion

Stellen Sie sich vor, Sie wären ein Bekleidungshändler betreiben seit vielen Jahren einen erfolgreichen Webshop mit WordPress und einem Shop-Plugin. Eines Tages häufen sich Kundenbeschwerden, Ihr Shop sei nicht erreichbar. Als Webmaster versuchen Sie sich in den Admin-Bereich einzuloggen. Sie werden auf ein Formular umgeleitet, welches Ihnen anzeigt, dass Ihre Website gesperrt worden sei und Sie diese gegen Zahlung eines Lösegeldes in Bitcoin wieder entschlüsseln können.

Die Website wurde von Ransomware gesperrt (Quelle: Wordfence)

Hintergrund Ransomware

Ransomware versucht über bekannte Sicherheitslücken in Systeme einzudringen und diese etwa durch Sperren, Verschlüsseln oder sogar Löschen unbrauchbar zu machen. Für die Freigabe sollen die Betreiber Lösegeld zahlen. Unsichere Websites befällt Ransomware meist, um sich weiter zu verbreiten – aber nicht immer. Zum Beispiel begann die Erpressersoftware CTB Locker, die ab 2014 zahlreiche Rechner v. a. in Westeuropa, Nordamerika und Australien infiziert hatte, 2016 auch Websites zu verschlüsseln, v. a. mit WordPress-Installationen. Die Malware „EV Ransomware" zielt ausschließlich auf WordPress. Der 2019 aufgetauchte Cryptovirus „B0r0nt0K" infiziert dagegen Linux-Webserver, verschlüsselt Dateien und Datenbanken und fordert 20 Bitcoin Lösegeld (das sind Stand April 2020 über 130.000 Euro).

Die Folgen ohne Sucuri

Als Webmaster wissen Sie, dass Sie auf die Forderungen der Erpresser nicht eingehen sollten. Sie versuchen daher, die Installation zu bereinigen. Wie Sie herausfinden, hat die Malware „EV Ransomware" tatsächlich zahlreiche Dateien auf dem Webserver verschlüsselt – darunter leider auch geschäftskritische Daten und sämtliche Backups, die nicht extern gespeichert worden waren. Den Shop neu aufzusetzen ist daher keine Lösung. Als Shop-Betreiber entscheiden Sie sich, das Lösegeld zu bezahlen. Tatsächlich haben Sie Glück und bekommen von den Erpressern einen Schlüssel zugeschickt. Wie sich aber herausstellt, funktioniert die Entschlüsselungsfunktion auf dem Erpresserformular nicht. Deshalb wenden Sie sich an einen externen Dienstleister, der Ihnen die Entschlüsselungsalgorithmen in PHP implementiert und mit Hilfe des Schlüssels tatsächlich die Website wiederherstellen kann. Der Vorfall verursacht einen Komplettausfall Ihres Onlineshops über mehrere Tage. Zudem wird die Website von Google auf die Blacklist gesetzt, was Sie als

Webmaster erst spät erfahren. Deshalb bleibt die Seite auch nach der Wiederherstellung längere Zeit nicht erreichbar.

Die Lösung mit Sucuri Website Security

Da Sucuri die Website regelmäßig serverseitig und remote auf Malware scannt, wird die Infektion frühzeitig erkannt und Sie als Webmaster automatisch benachrichtigt. Sie können sofort den Auftrag zur Bereinigung erteilen, damit das Sucuris Security Incident Response Team Arbeiten an der Website durchführen darf.

Die Security-Experten von Sucuri werden innerhalb weniger Stunden aktiv. Weil der Backup-Dienst von Sucuri Ultimate Dateien und Datenbanken automatisch auf externen Servern speichert, können diese die Website komplett wiederherstellen. Gleichzeitig überprüfen sie alle wichtigen Blacklist-Anbieter, um eventuelle Blacklistings entfernen zu lassen. Weil aber die Infektion schnell erkannt wurde, sind noch keine Blacklisteinträge erfolgt.

Außerdem checken die Spezialisten das System auf Schwachstellen, um eine Reinfektion auszuschließen. Die Ursache für den Ransomware-Befall war ein anfälliges WordPress-Plugin. Weil der Entwickler dafür noch kein Sicherheitsupdate bereitstellt, wird in der Sucuri Firewall ein virtueller Patch eingerichtet.

Noch am Tag der Infektion ist der Webshop vollständig wiederhergestellt. Ihnen als Betreiber des Onlineshops sind dadurch keine zusätzlichen Kosten entstanden und Sie sind zukünftig noch besser geschützt.

Praxisbeispiel 2: Verfügbarkeit am Black Friday sichern

In der „Black Week“ mit ihren Höhepunkten Black Friday und Cyber Monday verzeichnen Onlinehändler immer neue Umsatzrekorde. Das birgt nicht nur Chancen, sondern auch Gefahren: Onlineshops müssen in dieser Zeit auch bei hohem Ansturm besonders stabil laufen. Denn danach ist bereits ein großer Teil des Weihnachtsgeschäfts gelaufen.

Sie als Shop-Betreiber haben signifikant in Werbung investiert, um auf Ihre Sonderangebote an Black Friday und Cyber Monday aufmerksam zu machen. Diese treffen tatsächlich auf großes Interesse – Ihre Website verzeichnet schon Tage vor dem Black Friday so viele Zugriffe, dass die Antwortzeiten immer länger werden. Dann erhalten Sie eine Mail von Kriminellen: Wenn Sie nicht eine hohe Summe überweisen, wollen diese am Black Friday Ihren Webshop mit einem DDoS-Angriff komplett lahmlegen.

Die Folgen ohne Sucuri

Als Onlinehändler erkundigen Sie sich bei Ihrem Hoster, ob Sie kurzfristig für einige Zeit in einen performanteren Tarif wechseln können. Das geht, und deshalb entschließen Sie sich, den Erpressern nichts zu zahlen. Durch den Tarifwechsel ist der Shop einige Stunden nicht erreichbar, aber am Morgen des Black Friday wieder online. Im höheren Tarif kommt der Shop mit den steigenden Zugriffszahlen etwas besser zurecht. Dann machen die Kriminellen ernst: Am späten Vormittag erfolgt die erste Angriffswelle mit einer Bandbreite von ca. 20 Gbit/s. Der Netzwerkverkehr bricht ein, nur noch wenige Transaktionen können abgeschlossen werden. Weitere Wellen mit Bandbreiten bis zu 50 Gbit/s folgen am Nachmittag und gegen 20 Uhr. In diesen Zeiten ist Ihre Seite oft gar nicht mehr erreichbar. Auch nach der letzten DDoS-Welle erholt sich der Traffic nicht mehr; potenzielle Käufer sind inzwischen bei der Konkurrenz fündig geworden.

Die Lösung mit Sucuri Website Security

Sie als Onlinehändler buchen bei Ihrem Hoster DomainFactory das Security-Paket Sucuri Deluxe. Nun können Sie den angekündigten DDoS-Angriffen entspannt entgegensehen.

Sucuri nutzt ein weltweites Netzwerk von High-Performance-Servern mit eigenen DNS-Diensten, um zu jeder Zeit eine hohe Verfügbarkeit der geschützten Websites zu gewährleisten. Das cloudbasierte CDN verfügt über genügend Bandbreite, um auch massive Angriffe abzuwehren. Gleichzeitig bietet Sucuri damit auch genug Reserven, um saisonale Lastspitzen von regulären Anfragen zu bewältigen.

Die Sucuri Firewall überwacht zudem den kompletten Netzwerkverkehr und kann deshalb bösartige Anfragen erkennen und ausfiltern. Sie blockiert jegliche DDoS-Angriffe – auf Netzwerk- ebenso wie auf Anwendungsebene. Dazu bietet sie einen Echtzeitschutz vor den verschiedensten Cyber-Bedrohungen einschließlich Hacker-, Malware- und Brute-Force-Angriffen. Der Schutz wird ergänzt durch die ständige Überwachung auf Malware und andere Probleme. Mit dem Sucuri Vertrauenssiegel zeigen Sie Ihren Kunden, dass deren Daten bei Ihnen sicher sind.

Sucuri-Sicherheitsfunktionen

Sucuri Website Security bietet Ihnen einen Rundum-Sorglos-Schutz für Ihre Webanwendung: von der Erkennung und Beseitigung von Kompromittierungen über den vorbeugenden Echtzeitschutz und die Optimierung von Verfügbarkeit und Performance bis hin zu Absicherung durch automatische Backups.

Überwachung: Erkennung von Malware und Blacklisting

Ein leistungsfähiges Intrusion Detection System überwacht Websites per Remote & Server Side Scans ständig auf Anzeichen für Kompromittierungen (Indicators of Compromise):

- Malware-Infektionen
- Verfügbarkeitsprobleme
- SEO-Spam
- Blacklist-Status
- SL-Zertifikate
- DNS-Einstellungen

Schnelle Reaktion: Professionelle Malware-Bereinigung

Bei Malware-Problemen können Sucuri-Kunden ohne Mehrkosten eine professionelle Bereinigung durch Sucuris Malware-Profis beauftragen:

- Gründliche Analyse durch Spezialisten
- Nachhaltige Bereinigung aller Webseiten
- Entfernen von Malware, Backdoors, Defacements, SEO-Spam etc.
- Wiederherstellung der vollen Funktionsfähigkeit
- Löschung von Blacklisting-Einträgen
- Reaktion nach spätestens 30 Minuten (Tarif „Express“)

Sucuri Firewall: Prävention in Echtzeit

Die cloudbasierte Sucuri Firewall (Website Application Firewall / Intrusion Prevention System) filtert als Reverse Proxy alle eingehenden HTTP/HTTPS-Anfragen:

- Abwehr von Malware- und Hacker-Angriffen per SQLI, XSS, RFI/LFI etc.
- Schutz vor Zero-Day-Exploits
- Blockade von DDoS-Attacken
- Abwehr von Brute-Force-Attacken
- Virtual Patching & Hardening
- Zugriffskontrolle für sensible Seiten (IP-Whitelisting)
- Geoblocking
- Virtual Patching & Hardening

Content Delivery Network: Optimierte Verfügbarkeit und Performance

Ein global verteiltes Content Delivery Network mit Knoten in den USA, Europa, Asien, Australien und Brasilien erhöht die Website-Performance um durchschnittlich 70 Prozent:

- 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 im Notfall

Der Backup-Service von Sucuri speichert auf Wunsch automatisch alle Website-Dateien und Datenbanken:

- Automatische Backups für 90 Tage
- Täglich, wöchentlich, monatlich
- Speicherung auf hochsicheren Servern außerhalb der Hosting-Umgebung
- Exakte Wiederherstellung einer sauberen Installation

Sucuri Website Security: Tarifoptionen

Passende Pakete für unterschiedliche Anforderungen

Als DomainFactory-Kunde können Sie aus vier unterschiedlichen Sucuri-Tarifen wählen. Damit nutzen und zahlen Sie nur die Sicherheitsfunktionen, die Sie für Ihren Webshop oder Ihre Online-Anwendung benötigen.

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 Website-Betreiber 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