Stephan Czysch, Benedikt Illner

»Web Security – so sichern Sie Ihre SEO-Rankings

Die Kontrolle über die eigene Webseite zu verlieren, ist der Albtraum eines jeden Webmasters. Durch den gezielten Einsatz von Cloaking und die Platzierung versteckter Links kann es Angreifern gelingen, Ihnen und Ihrem Projekt nachhaltig zu schaden. Die daraus resultierenden Folgen reichen von Rankingverlusten bis hin zur vollständigen Entfernung Ihrer Webseite aus dem Suchmaschinenindex. Doch auch Ihre Reputation kann spürbaren Schaden nehmen. Wir wollen in unserem Artikel Möglichkeiten aufzeigen, wie Sie einen Befall entdecken können und welche Gegenmaßnahmen Sie bei einer Infizierung Ihrer Webseite ergreifen sollten.

DER AUTOR

Benedikt Illner ist Geschäftsführer der Online-Marketing-Agentur Trust Agents (*www.trustagents.de*). Als ausgebildeter Softwareentwickler kennt er die Gefahren für Webanwendungen und IT-Systeme.

DER AUTOR

Stephan Czysch verantwortet die Suchmaschinenoptimierung beim Berliner Startup Wimdu (*wimdu.de*). In den letzten Jahren war er als SEO-Strategieberater für weitere Gründungen von Rocket Internet aktiv.

Schwachstellen und Angriffspunkte

Der erste Anlaufpunkt für einen möglichen Angriff auf Ihre Webseite ist der Webserver, auf dem diese gehostet wird. Viele Angreifer machen sich dabei die ungenügenden Sicherheitseinstellungen des Systems zunutze oder gelangen durch eine zum Teil fehlerhafte bzw. veraltete Konfiguration des Servers direkt in das System. Mithilfe sogenannter Exploits, also im Prinzip Fehlfunktionen des Webservers, gelingt es ihnen, die vorhandenen Schutzmaßnahmen auszuhebeln. Leicht zu reproduzierende Benutzerdaten und einfache Passwörter oder generell falsch gesetzte Benutzerrechte beim Erstellen oder Hochladen von Dateien und Verzeichnissen ermöglichen Dritten ebenfalls den vereinfachten Zugang zu Ihren Dateien. Selbst wenn Sie sich nicht um die Pflege und Wartung des Servers kümmern und einen der vielen Webserver- bzw. Webhostinganbieter nutzen, sollten Sie sich keinesfalls zu sicher fühlen. Viele Provider aktualisieren ihre Server in sehr unregelmäßigen Abständen und reagieren nicht immer sofort, wenn ein neuer Exploit aufgedeckt wird.

Wurden serverseitig genügend Vorkehrungen getroffen, so sind es Webanwendungen, die den Hackern über meist ungewollte und unbemerkte Fehler in der Software einen erweiterten Zugriff ermöglichen. Weitverbreitete Content-Management-Systeme wie WordPress, TYPO3 und Drupal sind dabei ebenso wenig vor Sicherheitslücken geschützt wie aktuelle Shopsysteme, beispielsweise Magento und xt:Commerce. Vor allem aber durch die zahlreichen Erweiterungen, Templates und Plugins, die oft unbedarft installiert werden, erhöht sich das Sicherheitsrisiko eines solchen Systems um ein Vielfaches. Ihnen muss bewusst sein, dass jeder in Eigenregie Erweiterungen erstellen und somit unbemerkt mit Schadcode versehen kann. Auch bestehende Templates und Plugins können beliebig verändert und anschließend wieder zum Download angeboten werden. Ohne Kenntnis hat sich der Webseitenbetreiber somit eventuell einen unangenehmen und ungebetenen Gast in sein System geholt. Eigenentwicklungen und Anwendungen, die speziell für Sie erstellt wurden, sind von Hause aus mitunter sicherheitsanfälliger, da diese nicht von der breiten Masse verwendet und vor allem getestet werden. Die Aktualität der verwendeten Software, egal, ob Open-Source-Produkt oder kostenpflichtiges Tool, muss deshalb als wichtigstes Kriterium für einen hohen Sicherheitsstandard angesehen werden.

Die größten Gefahren, die von fehlerhaften Codebausteinen (unabhängig von bereits eingeschleustem Code) in Webanwendungen ausgehen können, sind das Cross-Site-Scripting* (XSS) und die sogenannten SQL-Injections*. Beide Angriffsmöglichkeiten nutzen die Tatsache aus, dass Benutzereingaben oder diverse Parameter (z. B. in den URL) nicht korrekt validiert werden. Beim XSS gelingt es dem Angreifer, unter anderem Skriptcode in eine bestehende Seite zu implementieren, zum Beispiel über einen

* siehe Glossar Seite 112-114

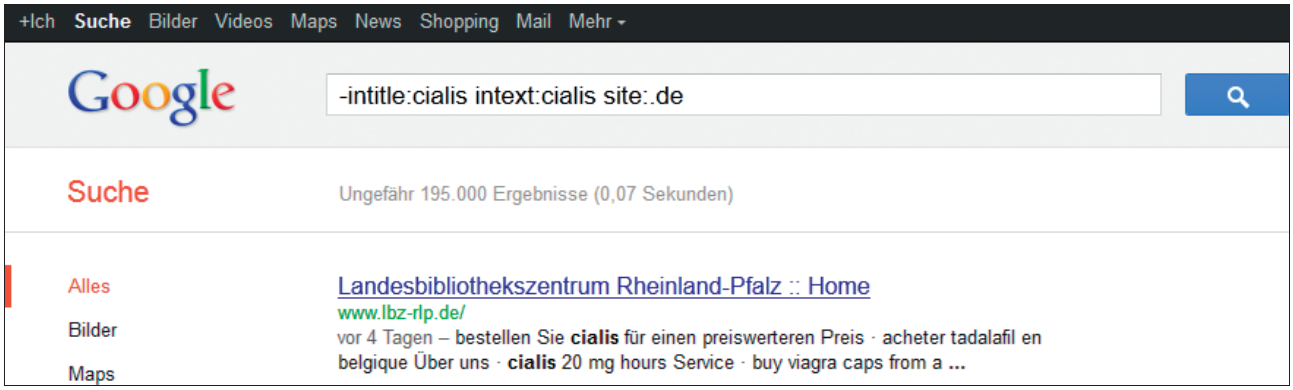


Abb. 1: Ausschnitt der Ergebnisseite für eine gezielte Suche nach veränderten Inhalten

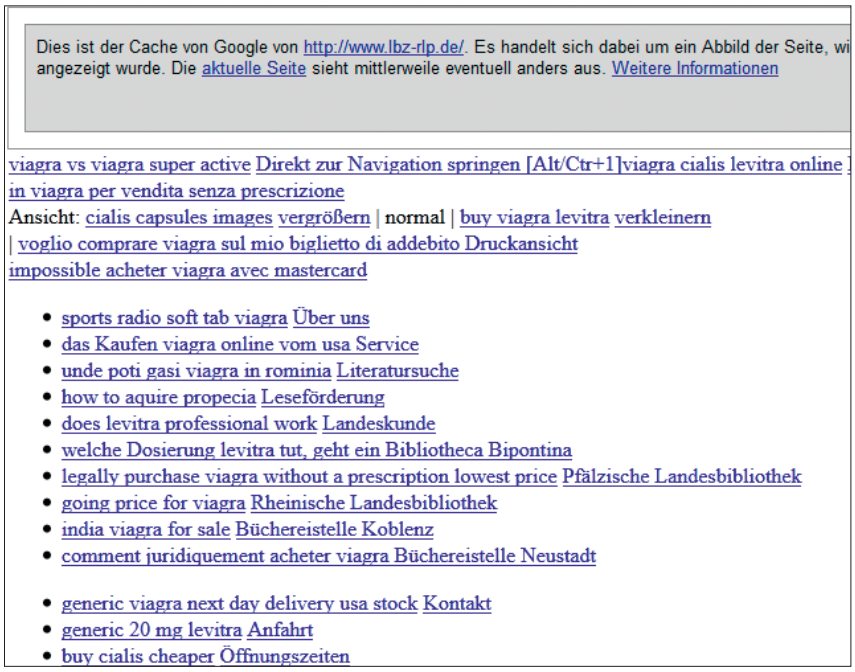


Abb. 2: Textversion des Google Caches für die Startseite von lbz-rlp.de

Kommentar in einem Blog oder einen Eintrag in das Gästebuch. Dieses Vorgehen wird oft verwendet, um ahnungslose Benutzer und deren Computer mit gefährlichem Schadcode zu infizieren. Des Weiteren könnten Angreifer die Inhalte Ihrer Webseite über iframes* negativ beeinflussen oder Phishing-Angriffe auf Ihre Besucher starten. Eine SQL-Injection zielt im Speziellen auf nicht validierte SQL-Statements ab, also Abfragen, die von der Anwendung an eine Datenbank gerichtet werden. Dabei reichen die Folgen eines solchen Angriffs vom Verändern des Contents Ihrer Seite bis hin zum Diebstahl wichtiger Kunden- und Benutzerdaten.

Ist ein Webauftritt erst einmal infiziert, so haben die Angreifer darüber hinaus eine Vielzahl an weiteren Möglichkeiten, um Ihnen zu schaden und für sich selbst Vorteile zu erwirtschaften. Zwei beliebte und weitverbreitete Methoden sind das Cloaking und der Einsatz von Hidden Links.

Cloaking – Ich sehe was, was du nicht siehst!

Cloaking bedeutet, dass bei unterschiedlichen Zugriffen auf die Seite, beispielsweise durch Suchmaschinen oder normale Besucher, abweichende Versionen der Webseite ausgeliefert werden. Dadurch ist es möglich, der

> „Kein System bietet hundertprozentigen Schutz vor Angriffen."

Suchmaschine beispielsweise einen Text über Sport zu zeigen, während Nutzer unter derselben Adresse Informationen über z. B. Hundezubehör bekommen. Besonders häufig werden auf infizierten Seiten Inhalte aus dem Adult- und Pharmazie-Bereich verbreitet.

Abbildung 1 zeigt ein solches Beispiel: Auf der Webseite des Landesbibliothekszentrums Rheinland-Pfalz www.lbz-rlp.de scheint es einem Angreifer gelungen zu sein, eigene Inhalte zu platzieren. Zumindest ist es schwer vorstellbar, dass die in dem Snippet, also der kleinen Beschreibung im Suchergebnis, gezeigten Wörter von den Betreibern des Webauftritts – zudem noch in unterschiedlichen Sprachen – verwendet wurden.

Je nach Zugriffsszenario auf die Seite reagiert der Webserver anders auf die Anfrage. So wird ein Nutzer, der nach dem Landesbibliothekszentrum Rheinland-Pfalz sucht oder die Webseite direkt über die Eingabe des Domainnamens oder eines Lesezeichens betritt, keine Veränderung auf der Webseite feststellen können und damit auch die im Snippet angezeigten Wör-

* siehe Glossar Seite 112-114

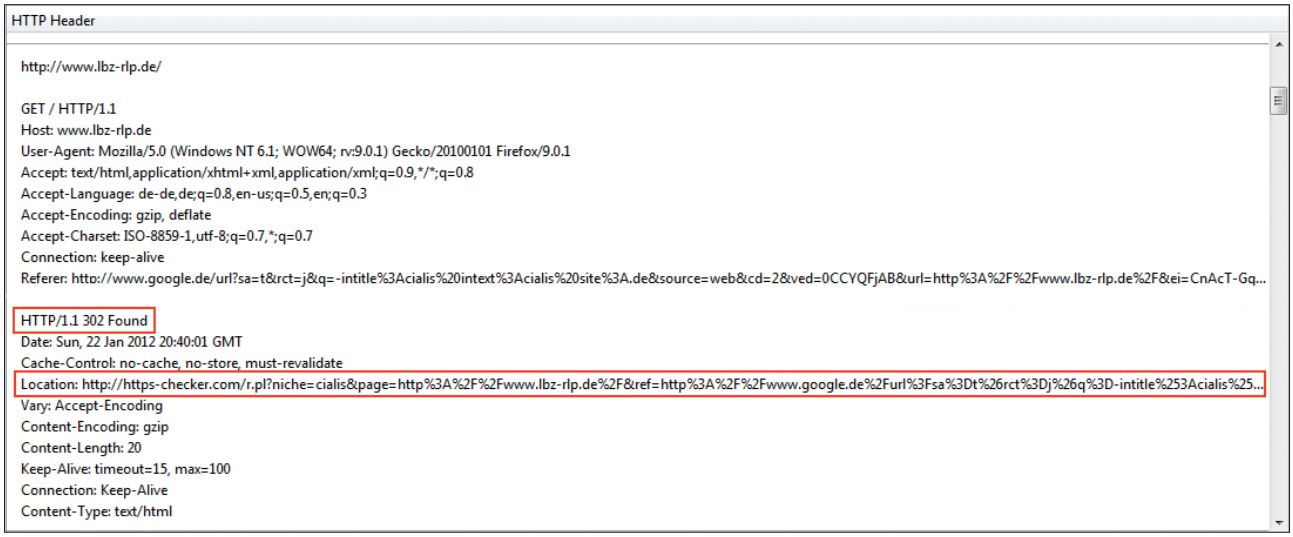


Abb. 3: Mitschnitt des HTTP-Headers* (mithilfe des „Live HTTP Headers“ Firefox Addons)

> „Wichtig: Achten Sie stets auf die Aktualität der verwendeten Software!“

ter nicht finden.

Wird die Webseite über die in der Abbildung 1 gezeigte Suchanfrage besucht, sieht man den Inhalt ebenfalls nicht. Dies liegt daran, dass man zu einem Webshop geleitet wird, der das im Snippet genannte Produkt vertreibt. Folglich scheint der Webserver einzig und allein für Suchmaschinenrobots den entsprechenden Inhalt auszuliefern und anzuzeigen. Und in der Tat: Wenn man sich die im Cache gespeicherte Version der Seite als Text-Version anzeigen lässt, sieht man die im Snippet angezeigten Textteile (siehe Abbildung 2).

Betrachtet man anstelle der Textversion die Seite im sogenannten „vollständigen Modus“ des Google Caches, sind die Links schwieriger zu finden, denn über eine Stylesheet-Angabe werden die Links für Benutzer nicht sichtbar auf der Seite dargestellt, obwohl sie im Quelltext vorhanden sind. Erreicht wird dies in diesem Beispiel über die Angabe

`<style>.oyli7s01 {visibility: hidden; } </style>` im Head-Bereich der Seite.

Für den Webseitenbetreiber bedeuten diese Links ein großes Risiko. Zum einen wird aktiv (wenn auch vom Webseitenbetreiber ungewollt) Cloaking betrieben, was gegen die Richtlinien der Suchmaschinen verstößt (Link zu trustagents.net/cloaking) und zu einem Ausschluss der Seite aus dem Suchmaschinenindex führen kann. Als prominentes Beispiel ist hier BMW zu nennen, die im Jahr 2006 aufgrund der aktiven Verwendung dieser Technik nicht mehr über die Google-Suche gefunden werden konnten (Link zu trustagents.net/bmw). Zum anderen wird der Besucher unter gewissen Voraussetzungen direkt auf eine andere Webseite geleitet, was je nach Geschäftsmodell Umsätze kostet und, nicht zu vergessen, der Reputation schaden kann. Und als wären diese Risiken nicht schon schlimm genug , wird die eigene Webseite thematisch in einen ganz anderen Bereich gerückt. So kann es passieren, dass die eigene Seite als “Adult” eingestuft wird und entsprechend in den Suchmaschinen nicht mehr so prominent für allgemeine Suchbegriffe zu finden ist.

In diesem Zusammenhang sollten wir noch einen kurzen Blick auf die Weiterleitung werfen, die Benutzer in Einzelfällen auf verschiedene externe Zielseiten leitet. Die Abbildung 3 zeigt einen kleinen Ausschnitt des HTTP-Headers. Der Antwortcode des Servers sowie die neue Location wurde rot markiert.

Auf die Anfrage nach der Startseite www.lbz-rlp.de antwortete der Server in diesem Fall mit „302 Found“, einer Weiterleitung, die den Nutzer nach einigen weiteren Zwischenschritten schließlich auf einen Webshop der Angreifer leitet. Bücher sucht man auf der Seite vergeblich - dafür kann man sich an einer reichlichen Auswahl pharmazeutischer Produkte erfreuen. Ein nicht wünschenswertes Szenario.

Mehr zum Thema Cloaking finden Sie hier (*http://einfach.st/cloak*).

Hidden Links

Mit dem Beispiel der Landesbibliothek haben wir auch direkt ein zweites Thema angeschnitten: Hidden Links. Vor einigen Jahren war das Verstecken von Text durch Auswahl derselben Farbe für Hintergrund und Text eine gängige Methode, um sich Vorteile in Suchmaschinen zu erschleichen. Mit auf Keyworddichte optimierten Texten wollte man Nutzer nicht belästigen – von daher machte man den Text unsichtbar. Hidden Links schlagen die-

* siehe Glossar Seite 112-114

Abb. 4: Hinweis auf die Manipulation einer Webseite in den Suchergebnissen

selbe Richtung ein: Für den Nutzer sind sie auf den ersten Blick nicht zu erkennen. Entweder werden die Links über Styleangaben nicht angezeigt oder in iFrames geladen. Suchmaschinen tolerieren Hidden Links nicht (Link zu trustagents.net/hiddenlinks). Wie schon beim Cloaking droht der Ausschluss aus dem Suchmaschinenindex und damit der schmerzliche Verlust von Besuchern aus Suchmaschinen.

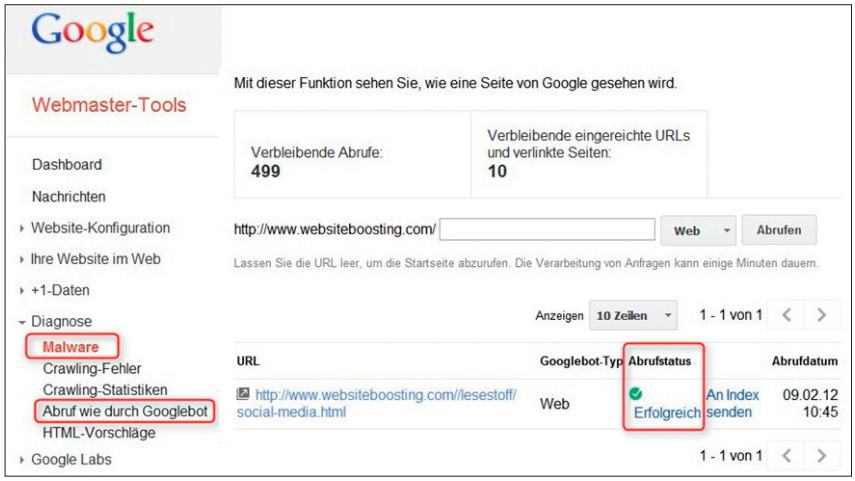
Um einen Einzelfall scheint es sich übrigens bei unserem gezeigten Beispiel nicht zu handeln. Stolze 193.000 Seiten werden von Google als Ergebnis zu unserer Abfrage (Abbildung 1) gelistet. Bei einer Vielzahl der vorzufindenden Resultate handelt es sich dabei um Webseiten, die mit TYPO3 betrieben werden, dem System, welches unsere Beispielseite nutzt. Die Angreifer machen sich anscheinend eine Schwachstelle in älteren Versionen des Content-Management-Systems zunutze, um sich gezielt im System festzusetzen.

Ist Ihre Webseite auch betroffen? So machen Sie den Check

Eines vorweg: Im Kampf gegen Webspam und Malware sind Sie nicht allein. Besonders Google hilft Webseitenbetreibern und Internetusern, Gefahren für den eigenen Computer oder die eigene Webseite zu minimieren.

Ein sehr wichtiges und nützliches Tool, nicht nur für Web Security, sind die Webmaster-Tools von Google (Link zu trustagents.net/wmt). Nach erfolgter Authentifizierung des eigenen Webauftritts bekommen Sie über die Webmaster-Tools Nachrichten zugestellt, wenn Google Probleme mit Ihrer Webseite festgestellt hat. Unser Tipp: Lassen Sie sich Nachrichten, die Sie über die Webmaster-Tools erhalten, immer an eine E-Mail-Adresse weiterleiten, die Sie regelmäßig kontrollieren. Die nötige Einstellung nehmen Sie direkt in den Webmaster-Tools unter (Link zu *trustagents.net/ wmtsettings*) vor.

Besondere Beachtung sollten Sie den Punkten „Malware“ und „Abruf wie durch Googlebot“ schenken, die Sie in der Navigation unter „Diagnose” finden können. Ersteres gibt Ihnen einen Hinweis aus, wenn Schadcode auf Ihrer



Die Google Webmaster-Tools zeigen an, ob eine Website mit schadhaftem Code manipuliert wurde

Abb. 5: Achtung! Diese Webseite kann Ihren Computer gefährden

Seite gefunden wurde, und Letzteres zeigt Ihnen den HTML-Code, den Google auf Ihrer Seite ausgeliefert bekommen hat. Sollten Sie hier Elemente – ob Text oder Links – entdecken, die Sie selbst nicht auf der Seite finden, kann dies ein Hinweis auf eine Infizierung Ihrer Webseite sein. Darüber hinaus befindet sich im Labs-Bereich der Webmaster-Tools aktuell ein Feature namens „Vorschau" bzw. „Preview", mit dem Sie ganz einfach einen Snapshot Ihrer Seite erstellen lassen können, um etwaige Versionsunterschiede zwischen Mensch und Maschine auf einen Blick zu erkennen.

Auch die Google-Websuche ist ein mächtiges Werkzeug, um den Status Ihrer Webseite zu überprüfen. Um Schaden von Besuchern einer Webseite abzuwenden, macht Google auf gefundene Probleme direkt inmitten des Suchergebnisses aufmerksam (siehe Abbildung 4).

Um zu kontrollieren, ob auch für Ihre Webseite eine solche Warnung ausgegeben wird, sollten Sie die Abfrage site:ihrewebseite.de in Google starten. Beachten Sie hierbei, dass nur einzelne Seiten Ihrer Webseite betroffen sein können. Nehmen Sie sich daher die Zeit, den Status Ihrer Webseite, also vor allem auch gezielt die Unterseiten, genau zu kontrollieren. Sollten Sie bei der Abfrage fündig werden, ist es spätestens dann Zeit, zu reagieren! Denn nicht nur Sie sehen diese Nachricht, sondern auch alle Googlenutzer, die sich für Ihre Seite interessieren. Und verlorenes Vertrauen wiederzugewinnen, ist nicht einfach.

Wie bereits im Praxisbeispiel gezeigt, ist die Verwendung des Googles Caches als Textversion ein ebenso nützliches Werkzeug, um versteckte Inhalte sichtbar zu machen. Wir empfehlen ebenfalls, eine Site-Abfrage für Ihre Webseite durchzuführen und anschließend die indexierten Seiten mithilfe des Caches genauer zu untersuchen.

Eine Stufe über der einfachen Manipulation steht die Meldung, dass die betroffene Webseite dem Computer schaden kann. In diesem Zusammenhang wird dem einen oder anderen folgende Nachricht bekannt vorkommen, vorausgesetzt, Sie surfen mit Firefox oder Googles Chrome. Nach dem Öffnen einer infizierten Seite erhalten Sie einen Hinweis wie er in Abbildung 5 zu sehen ist.

Neben der Meldung auf der Seite wird auch in der Google-Suche ein ähnlicher Hinweis unterhalb der URL angezeigt. Doch was heißt es, wenn eine Webseite als attackierend eingestuft wurde? In einem solchen Fall geht die Manipulation über das noch harmlos anmutende Einfügen von Links und Texten hinaus – die Webseite wird dazu missbraucht, Schadcode weiterzuverbreiten. Ob Ihre Webseite betroffen ist, können Sie dabei auch unter *http://einfach.st/sbad* in Erfahrung bringen.

Übrigens bittet Google auch um Mithilfe: Wenn Sie schadhafte Webseiten finden, können Sie diese melden (*http://einfach.st/badw*). Einen weiteren Check über den Gesundheitszustand Ihrer Webseite können Sie unter *www.google.com/safebrowsing/diagnostic?site=IhreWebseite.de* durchführen, wobei man „IhreWebsite.de" selbstverständlich mit der eigenen Domain ersetzen muss.

So werden Sie den Eindringling wieder los

Ist Ihre Webseite erst einmal befallen, sollten Sie diese temporär vom Netz nehmen. Wir empfehlen Ihnen zudem, den HTTP-Statuscode 503 zu senden, der für Wartungsarbeiten verwendet werden soll. So schmerzhaft das Abschalten der eigenen Seite auch sein mag – die Sicherheit und der Ruf Ihrer Webseite sollten im Vordergrund stehen.

Anschließend sollten Sie alle besteheden Zugangsdaten für Ihren Server abändern. Schwierig wird natürlich die Suche nach der Schwachstelle im System. Schauen Sie zunächst auf Ihrem Webserver nach, ob Sie Dateien finden, deren Herkunft Sie nicht validieren können oder deren Aktualisierungsdatum eventuell auffällig ist. Wenn Sie die ungefähre Position des Schadcodes auf Ihrer Webseite identifizieren konnten, sollten Sie besonders die entsprechenden Codebestandteile untersuchen. Im Idealfall finden Sie den eingeschleusten Code schnell und können ihn daraufhin einfach entfernen.

> „Regelmäßige Sicherheitskopien helfen, mögliche Schadensfälle einzudämmen."

Beim Entfernen des Schadcodes sind mitunter auch die Google-Webmaster-Tools hilfreich. Unter dem Punkt Diagnose – Malware sehen Sie Infektionen, die von Google auf Ihrer Webseite gefunden wurden. Dort können Sie nach dem erfolgten Entfernen der Infektion eine erneute Überprüfung Ihrer Webseite auf Malware anstoßen. In manchen Fällen ist auch ein Antrag auf eine erneute Überprüfung der Webseite nötig, der sogenannte „Reconsideration request".

Idealerweise belassen Sie es nicht nur beim Entfernen des Codes, sondern installieren die von Ihnen genutzte Webapplikation in der aktuellsten Version neu. Die Schreibrechte auf Dateien und Ordner passen Sie im Anschluss nur wie vom Softwarehersteller vorgegeben an. Auch ein Update des Webservers ist in manchen Fällen ratsam. Wenn Sie den Webserver nicht selbst betreuen, sollten Sie Ihren Webhostinganbieter kontaktieren. Sichern Sie zuvor aber Datenbanken und vom Sys-

Tipp:

Die Folgen eines von Fremden manipulierten Webservers können fatal sein. Google nimmt nicht nur sofort die komplette Domain aus den Rankings, sondern sperrt sie auch für AdWords-Anzeigen, um Suchende zu schützen. Ist man als Shopbetreiber auf einen stetigen Kundenstrom über Google angewiesen, bleibt ab diesem Moment der Umsatz aus. Entfernt man dann alle Manipulationen, bedeutet das noch lange nicht, dass die Domain Minuten später wieder gefunden werden kann. Nach der Einreichung zur erneuten Überprüfung über die Webmaster-Tools kann es mehrere Tage oder gar Wochen dauern, bis die Sperre wieder aufgehoben wird. Gerade Shopbetreibern kann man daher nur empfehlen, einmal durchzurechnen, wie lange sie praktisch ohne Umsatz überleben können. Ist die Zeitspanne sehr kurz, rechnen sich durch die Risikominderung oder -vermeidung entsprechende Vorsichtsmaßnahmen recht schnell. Dem Vernehmen nach häuft sich das Hacken von Webservern in letzter Zeit spürbar. Und wie viele Server tatsächlich mittlerweile schon mit solchen Tricks infiziert wurden, kann niemand abschätzen. Versierte Hacker hinterlassen nur wenige Spuren und halten die Manipulationen eher gering. So haben sie gute Chancen, lange Zeit unentdeckt zu bleiben! *(Mario Fischer)*

tem unabhängige Uploads, um einen Datenverlust zu vermeiden. Wichtig: Bevor Sie die gesicherten Daten wieder einspielen, überprüfen Sie vor allem die Datenbank auf eventuelle Unregelmäßigkeiten. Seien Sie sich bewusst, dass Ihr Computer unter Umständen ebenfalls infiziert wurde und der Schadcode so wiederum erneuten Zugang auf Ihren Webserver nehmen kann. Wir empfehlen Ihnen daher, Ihre Daten regelmäßig zu sichern, um den möglichen Schaden und Verlust so gut wie möglich einzudämmen. Fragen Sie daher am besten direkt bei Ihrem Provider nach einer geeigneten Backuplösung für Ihre Dateien.

Zusammenfassend: Die Checkliste

» Überprüfen Sie vorhandene Sicherheitsvorkehrungen (Zugangsdaten, Berechtigungen)
» Halten Sie jegliche verwendete Software stets auf dem neuesten Stand
» Beziehen Sie Updates und Erweiterungen nur von autorisierten Quellen
» Erstellen Sie regelmäßig ein Backup Ihrer Webseite bzw. des ganzen Webservers
» Überprüfen Sie Ihre Webseite auf versteckte Inhalte oder Ihnen unbekannte Skripte
» Durchforsten Sie im Ernstfall alle Dateien auf Ihrem Server und verändern Sie die Zugangsdaten
» Bringen Sie ihre Webseite bei Bedarf vorübergehend in den Wartungsmodus
» Lassen Sie Ihre Seite nach abgeschlossener Bereinigung überprüfen

Eine Übersicht über nützliche Tools und Seiten zum Sicherheitscheck finden Sie unter *trustagents.net/website-boosting*

Fazit/Ausblick 2012

Sie sollten sich nicht der Illusion hingeben, dass Ihre Webseite das Fort Knox des Internets ist. Sicherheitslücken sind nur schwer vollständig auszuschließen und Ihre Aufgabe als Webseitenbetreiber ist es, die Gefahren eines Angriffs zu minimieren und potenzielle Schäden so gering wie möglich zu halten. In den vergangenen Monaten sind immer wieder Webseiten in das Visier Krimineller gelangt und auf absehbare Zeit wird sich dies leider nicht ändern. Man denke dabei nur an den Schuhgiganten Zappos, der in diesem Januar den Diebstahl von 24 Millionen Kundendaten eingestehen musste (Link zu trustagents.net/zappos).

Wie bei anderen IT-Bereichen auch sollten Sie mit Sicherheitsmaßnahmen nicht erst beginnen, wenn der Schaden bereits entstanden ist. Machen Sie sich rechtzeitig Gedanken und klopfen Sie Ihre Webanwendung auf Sicherheitslücken ab. Die dafür aufzubringenden Ressourcen lohnen sich – oder möchten Sie Ihren Kunden mitteilen, dass seine Daten aus Ihrer Datenbank extrahiert wurden? Neben einer leidenden Reputation ist auch der Verlust des wertvollen Besucherstroms aus Suchmaschinen ein gewichtiger Grund, in Web-Sicherheit zu investieren. Der Verlust von umsatz- und besucherbringenden Suchwörtern ist genauso schmerzhaft wie die vollständige Entfernung der eigenen Seite aus dem Index der Suchmaschinen. Unbestrittenerweise kann sich eine Seite von einer Zurückstufung erholen, dennoch fehlt in der Zwischenzeit bares Geld.

Aus diesem Grund empfehlen wir Ihnen nochmals nachdrücklich, die Google-Webmaster-Tools zu nutzen und die verwendete Software auf Ihrer Webseite stets aktuell zu halten. Überlegen Sie sich auch, woher Sie die Updates für Ihre Webapplikation beziehen, welchen Programmierern Sie vertrauen und ob Sie wirklich jedes Plugin brauchen, das Sie im Netz finden können. Selbiges gilt auch für Designs, die Sie über eine Vielzahl von Kanälen im Web finden können.¶