

Webseiten-Sicherheit für Anwender und Web-Administratoren

Klick ohne Risiko

Das World Wide Web ist ein gigantisches Sammelsurium an Informationen. Wer nur beharrlich sucht, wird auf fast jede Frage eine Antwort bekommen. Nur manchmal ist die vermeintliche Antwort auf einer Webseite zu finden, deren Macher ganz andere Interessen verfolgen als das, was die Seite selbst vorgibt. Der Besuch bestimmter Seiten reicht schon, um über die Mechanismen des Browsers gefährlichen Schadcode auf den Rechner gespielt zu bekommen. Daher ist es durchaus ratsam, die Webseite vor einem Besuch zu überprüfen. Aber selbst vertrauliche Webseitenanbieter mit den besten Absichten können zu Schadcode-Schleudern werden, wenn sie den Hackern versehentlich eine Tür offenhalten, über die sie bösartige Programme bei ihrem „Wirt“ einschleusen können. Wir stellen die wichtigsten Tools für Anwender und Administratoren vor, um sich selbst beziehungsweise die eigene Organisation vor solchen bösen Fallen beziehungsweise Attacken auf die eigene Web-Präsenz zu schützen.

Ein Programm kann man auf Schadsoftware überprüfen. Eine E-Mail auf SPAM-Content – aber wie überprüft man, ob eine Webseite sicher ist oder nicht? Viele Anwender besuchen eine Webseite einfach so, darauf hoffend, dass der Anbieter nur die besten Absichten hat. Leider geht das immer häufiger schief. Das muss aber nicht sein, denn es gibt einfache Mittel, die auch einen unerfahrenen Webseiten-Besucher beim Check von Webseiten unterstützen.

SiteAdvisor

Die Antivirus-Industrie bietet bereits clevere Lösungen an. McAfees Siteadvisor beispielsweise (<http://www.siteadvisor.de/>

download/windows.html#) blendet nach Installation eines zusätzlichen Browser-Plugins kleine Symbole im Browserfenster ein. Sucht der Anwender mittels einer Suchmaschine nach einer Webseite, werden alle angezeigten Ergebnisse von SiteAdvisor bewertet. Einstufungen sind dabei:

- Ungefährlich; Kein oder sehr geringes Risiko
- Vorsichtig; Niedriges Risiko
- Warnung; Erhebliches Risiko
- Unbekannt; Noch keine Bewertung – Bitte Vorsicht!

Wer kein Plugin installieren möchte, der kann eine einzelne URL-Adresse auf der Si-

teAdvisor-Webseite überprüfen lassen (<http://www.siteadvisor.de/>).

Secure Browsing

Der israelische Hersteller Finjan, der inzwischen zu M86 Security gehört, bietet eine ähnliche Funktionalität an. Auch Secure Browsing zeigt nach Installation als Browser-Plugin eine Bewertung der Webseite innerhalb von Suchergebnissen an. Analog zu SiteAdvisor ist auch hier eine Einzelprüfung (<http://www.finjan.com/Content.aspx?id=574>) einer URL-Adresse möglich, ohne das Plugin zu installieren.

Als Dritter im Bunde sei noch der Antivirus-Hersteller AVG genannt. Dessen Linkscanner (<http://www.linkscanner.de/>) bietet eine gleichwertige Funktionalität. Die Überprüfung einer einzelnen Adresse (<http://www.avg.com.au/resources/web-page-scanner/>) ist hier ebenfalls möglich.

SafeBrowsing/Google

Bereits seit längerem überprüft Google im Rahmen seiner Websitensuche auch den Malware-Zustand von Webseiten (verfügbar über die Google Webmaster-Tools). Wer den SafeBrowsing-Status mit dem Parameter „diagnostic“ abrufen, erhält den Malware-Status, so wie Google es sieht. Was ge-

Safe Browsing
Diagnosesite für www.secuteach.de Ratgeber - bereitgestellt von

Wie ist die gegenwärtige Einstufung von www.secuteach.de?
Diese Website ist gegenwärtig nicht als verdächtig eingestuft.

Welche Befunde hat Google beim Besuch dieser Website festgestellt?
Google hat diese Website in den letzten 90 Tagen nicht besucht.

Hat diese Website als Überträger zur Weiterverteilung von Malware fungiert?
In den letzten 90 Tagen hat www.secuteach.de anscheinend nicht als Überträger für die Infektion von Websites fungiert.

Hat diese Website Malware gehostet?
Nein, diese Website hat in den letzten 90 Tagen keine Malware gehostet.

Nächste Schritte:

- [Zur vorherigen Seite zurückkehren.](#)
- Falls Sie Eigner dieser Website sind, können Sie eine Überprüfung Ihrer Website mit den Google [Webmaster-Tools](#) anfordern. Weitere Informationen über den Prüfprozess erhalten Sie in der [Hilfe für Webmaster](#).

Updated 24 hours ago

Die Adresse <http://www.google.com/safebrowsing/diagnostic?site=IHREDOMAINURL> führt zur Überprüfung der Webseite, die anstelle des Platzhalters „IHREDOMAINURL“ angegeben ist.

nau Google überprüft, ist aktuell nicht hinterlegt. Man darf aber annehmen, dass sich die angebotene Funktionalität an den üblichen Suchmechanismen orientiert.

SAFEWEB

Auch Norton beziehungsweise Symantec hat einen Dienst für die Webseiten-Überprüfung im Angebot. Allerdings ist man dort etwas mitteilbarer und zeigt eine detaillierte Information, was genau geprüft wurde. Der Check ist über die Hauptseite von SAFEWEB (<http://safeweb.norton.com/>) aktivierbar. Webmastern, die ihre Seite via SAFEWEB bewertet haben möchten, sei angeraten, sich bei SAFEWEB anzu-

melden – es dauert sonst unter Umständen recht lange, bis die Webseite automatisch erstmalig geprüft wird.

Web Of Trust (WOT)

Bei WOT steht der Mensch im Vordergrund – denn Menschen vertrauen Menschen. So wird bei WOT kein Virens Scanner bemüht, sondern es sind die Besucher von Webseiten selbst, die den Seiten ihre Empfehlung aussprechen oder eben davor warnen. Der Gedanke dabei ist, dass eine Webseite, die mit Schadsoftware verseucht ist oder andere Risiken beherbergt, bei einer Interaktion durch den Menschen negativ auffällt. Mögliche Negativmerkmale sind etwa, dass ein lokal installierter Virens Scanner oder der Browser eine Warnmitteilung generiert. Oder aber, dass die Webseite mit Pop-Ups überladen ist, die mit dem eigentlichen Thema nichts zu tun haben. In diesen Fällen würde der Besucher eine schlechte Beurteilung erteilen.

Das WOT-System funktioniert umso besser, je mehr User sich daran beteiligen und je häufiger eine Webseite besucht wird. Sollte noch keine Beurteilung vorliegen, sollte man vorübergehend auf eine andere Überprüfungsmethode zurückgreifen. Über die WOT-Webseite (<http://www.mywot.com/de>) lassen sich einzelne URLs testen, man kann aber auch ein Browser-AddOn für IE oder Firefox downloaden und installieren. Die Vertraulichkeitsstufe der Webseiten wird dann im Browser angezeigt.

Hackalarm24

Hackalarm24 ist das Ergebnis der Kooperation zweier Unternehmen aus Österreich. Hackalarm überwacht Webseiten und Webshops auf erfolgte Hackerangriffe. Diese Funktion steht als kommerzielle

Dienstleistung zur Verfügung. Hackalarm24 erlaubt es auch, einzelne Webseiten zu überprüfen (http://www.hackalarm24.com/frontend/scripts/index.php?setMainAreaTemplatePath=mainarea_checkextern.html&groupid=200). Damit kann der Besuch einer Webseite oder eines Shops gesichert werden.

Unmask Parasites

Schlicht und effektiv präsentiert sich die Webseite von Unmask Parasites. Nach Eingabe einer URL wird die Webseite hinter der angegebenen Adresse auf Malware Scripts, Webseiten-Weiterleitungen oder versteckte Spam-Links überprüft (<http://www.unmaskparasites.com>). Wurden keine „Parasiten“ entdeckt, meldet Unmask Parasites „This page seems to be <clean>“ (zu Deutsch etwa: „Diese Seite scheint sauber zu sein“).

Da keine Überprüfung zu 100 Prozent garantieren kann, dass alle Computerviren, Manipulationen oder sonstige Angriffe entdeckt wurden, empfiehlt UP auch die Nutzung weiterer Dienste, um das Ergebnis zu sichern.

Sicherheit für Webseiten-Administratoren

Neben Marketing-, Grafik- und Content-Optimierung müssen Webseiten-Admins auch ein Auge auf die Unversehrtheit ihrer Webseite haben. Dies ist eine nicht zu unterschätzende Herausforderung, da mitunter bereits ein einziger Fehler im Content-Management-System, im Betriebssystem, in der Web-Anwendung oder im Webserver genügt, um einem Angreifer ein Schlupfloch zu bieten.

Entsprechend vielfältig ist dabei das Szenario. Einen Überblick über die bekannten Angriffsmethoden gibt es beim Web Application Security Consortium (<http://projects.webappsec.org/Threat-Classification>), das eine Threat-Klassifikation anbietet. Begriffe wie Cross-Site-Scripting, URL Redirector Abuse oder Server Misconfiguration sind hier entsprechend erklärt. Viele Anbieter offerieren hilfreiche Services für den sicherheitsbewussten Webseiten-Admin.

DASIENT

DASIENT hat sich auf Anti-Malware-Lösungen spezialisiert. Der Hersteller bietet automatisierte Scan-Vorgänge inklusive E-Mail-

Nutzen von Überprüfungen

Eine Webseiten-Analyse ist immer eine Momentaufnahme, die auf Basis einer definierten Teilmenge der bekannten Angriffsvarianten (Vulnerabilität, SQL-Injection, Schadsoftware etc.) beruht. Kein Service kann alle weltweit existierenden Angriffsvarianten erkennen. Dies geht unter anderem auch schon deshalb nicht, da in der Regel die Services von außen auf die Webseite zugreifen und damit nicht uneingeschränkt auf alle Daten Zugriff haben.

Trotzdem stellt die Überprüfung auf Schadsoftware eine wichtige Schutzmaßnahme dar. Denn die Gefahr, dass eine Webseite infiziert ist, nimmt stetig zu.

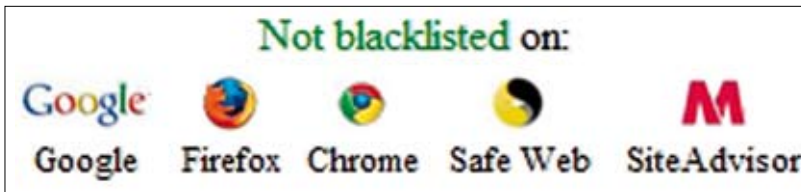
150 Webseiten ...

... muss man im Schnitt besuchen, um auf eine infizierte Seite zu gelangen. Das ergab die Beobachtung mehrerer hunderttausend Webseiten durch Kaspersky Lab. Erschreckende Tendenz: War 2006 im Schnitt nur eine von 20.000 Webseiten infiziert, so lauerte im Jahr 2009 bereits auf jeder 150. Seite eine Online-Bedrohung.

Über infizierte (manipulierte) Webseiten wiederum gelangt Schadsoftware zum Anwender, der damit unter Umständen seinen eigenen PC infiziert und so selbst zu einer Virus-Quelle wird. Ein verbesserter Schutz lässt sich aber nur erreichen, wenn die Überprüfung von besuchten Webseiten automatisch erfolgt. Denn kein Anwender wird den Zusatzaufwand betreiben und eine Webseite manuell überprüfen und auch folgerichtig entsprechend der erreichten Sicherheitsstufe handeln (Diese Webseite ist vermutlich manipuliert – wir raten von einem Besuch ab).

Daher lässt sich ein guter (Basis-)Schutz für den Anwender nur durch Browser-AddOns erreichen, die fest im Systemumfeld integriert sind, oder durch zentrale Sicherheitskomponenten wie beispielsweise Vulnerability- oder Schadsoftware-Scanner am Internet-Gateway.

Benachrichtigung auf Stunden-, Tages- oder Wochenbasis gegen Bezahlung an. Wer möchte, kann auch eine abgespeckte Gratis-Überprüfung nutzen, die einmal wöchentlich eine Webseite verifiziert. Hauptbestandteil dabei ist die Überprüfung, ob die Webseite auf einer Blacklist steht. Für diese Gratis-Prüfung ist eine Anmeldung erforderlich (<https://wam.dasient.com/wam/info?URL=Enter+your+Domain&scan=1&diagnose=1&prod=19&x=63&y=4>).



Hauptbestandteil der DASIENT-Überprüfung ist, ob die angegebene Webseite auf einer Blacklist steht.

SiteSecurityMonitor (SSM)

Ehemals bekannt unter dem Namen „54F3.com“ bietet SSM nun seine Dienste an. Ebenso wie DASIENT ist SSM auf den Sektor Schadsoftware spezialisiert (<http://www.sitesecuritymonitor.com/>). SSM sucht dabei nach mehr als 100.000 bekannten Malware-Codes und erkennt ergänzend dazu mehr als 32.000 Schwachstellen (Vulnerabilities).

German Web Security (GWS)

Im überwiegend von amerikanischen Herstellern dominierten Markt wirkt German Web Security durchaus etwas exotisch. Zusätzlich zum Gratis-Web-Scan-Service wird auch hier ein erweiterter Service gegen Bezahlung angeboten. GWS bietet darüber hinaus auch Dienstleistungen wie Pen-Testing und Webseiten-Codeoptimierung an (<http://www.german-websecurity.com/de/home/>). Der Gratis-Scan-Service vermittelt einen ersten Eindruck, wie sicher eine Webseite ist (allgemeine Daten werden angezeigt – Details müssen hinzugekauft werden).

McAfee SECURE

Die kommerzielle Version von McAfees SiteAdvisor ist SECURE (<http://www.hacker-safe.nl/info/?groep=de&pageid=100000126>). Die Zielgruppe von SECURE sind größere Webseiten-Betreiber und größere Webshops. SECURE offeriert ein Zertifikat, welches auf den Webseiten eingebunden werden kann und so dem Kunden/Besucher anzeigt: „Diese Webseite ist sicher“. Nach eigenen Angaben von McAfee wird SECURE

RE derzeit auf mehr als 80.000 Websites eingesetzt.

Online Link Scan

Abschließend sei noch eine einfache Variante erwähnt, die einen schnellen Check einer Webseite für den Administrator durchführt. Der Online-Link-Scan nutzt dabei verschiedene Anbieter additiv, um eine Webseiten-Einschätzung abzugeben (<http://onlinelinkscan.com/>). Dieser Service

muss manuell gestartet werden, ist dafür aber umsonst und jederzeit nutzbar.

Empfehlung für Web-Admins

Neben den hier erwähnten Online-Diensten gibt es noch weitere Anbieter am Markt (<http://www.acunetix.com/>, <http://www.gfi.com/lannetscan/free-network-security-scanner>, <http://www.merchant-safe.com/>, <http://sucuri.net/index.php?page=home> oder <http://www.qualys.com/>). Wichtig für den Webseiten-Administrator ist dabei, dass er bei Bedarf Unterstützung für seine Tätigkeit erhält beziehungsweise käuflich erwerben kann. Allerdings hat auch in diesem Umfeld Sicherheit durchaus ihren Preis. Wer einen Rundum-Service will, muss auch entsprechend tief in die Tasche greifen. Wer sich um einen professionellen Service für die Überwachung der eigenen Webseite kümmern möchte, sollte die Anbieter genau unter die Lupe nehmen. Kriterien zur Nachfrage sind beispielsweise:

- Was wird überprüft (Malware, Vulnerabilities, Codefehler, Web-Applikationen)?
- Wie häufig wird die Webseite überprüft (täglich, wöchentlich, einmalig)?
- Gibt es ein Sicherheits-Zertifikat, zur Darstellung auf der Webseite?
- Gibt es Anerkennungen für das Zertifikat/Siegel von dritter Seite?
- In welcher Tiefe wird die Webseite geprüft (nur die erste Seite oder alle Seiten)?
- Welche Reports werden in welcher Form (PDF, XML ...) erstellt?

- Sind die Validierungen nachvollziehbar beschrieben?
- Welche Preise gelten? Sind im Problemfall zusätzliche Scan-Läufe möglich?
- Gibt es eine GUI, zur Individualisierung von Scan-Parametern bzw. Scan-Umfang?
- Ist der Scan auf IP-Adressen oder Domain-Namen festgelegt?
- Gibt es Referenzkunden und Aussagen zur Scan-Qualität?
- Müssen Kennungen/Tools/Agenten etc. auf der Webseite installiert werden?
- Welche Webserver werden unterstützt (Apache, IIS etc.) bzw. untersucht?
- Wird der HTML-Code auf typische Fehler untersucht, wie sie zum Beispiel bei Verwendung bestimmter CMS (Content-Management-Systeme) oder Web-Editoren entstehen?
- Wie lange gibt es den Anbieter bereits am Markt?

Einen interessanten Service, der aktuell noch im BETA-Stadium ist, stellt URLVOID (<http://www.urlvoid.com/>) dar. URLVOID fasst mehrere Einzeldienste zusammen und stellt die Ergebnisse in übersichtlicher Form dar. Dabei hat der Service der NoVirusThanks Company das Potential, zu einem der Standardtools zu werden.

Wer sich am Markt umsieht, wird eine Lösung finden, die den jeweiligen Ansprüchen gerecht wird. Sicherheit ist wichtig – und wird auch im Web-Umfeld immer wichtiger und zunehmend zu einem Faktor, der über den Geschäftserfolg und die Online-Reputation entscheidet. ■



Ralph Dombach, freier Autor und Sicherheits-Administrator für einen Versicherungskonzern (www.secuteach.de; Twitter: secuteach)