HTTPS als Rankingfaktor: So geht das mit dem SSL-Zertifikat

–Gastbeitrag von Christian Heutger, Geschäftsführer der PSW Group–

Google möchte das World Wide Web sicherer machen – und aus diesem Grunde hat der Suchmaschinenriese nicht nur ein Sicherheitsteam aus hochrangigen Hackern zusammengestellt, sondern im Sommer 2014 bekanntgegeben, verschlüsselte Webseiten besser ranken zu lassen. Tilmann Klosa ging als SEO-Profi in diesem Artikel konkreter darauf ein, während wir uns für die Einladung zu diesem Gastartikel bedanken und aus Sicht der Security-Experten berichten möchten.

Großflächige Verschlüsselung: Welche Kritikpunkte sind korrekt?

Gefühlte Sicherheit – dieser Punkt ist für diverse Anwender ein Kriterium, sich gegen Verschlüsselung zu entscheiden. Es stimmt: Eine verschlüsselte Webseite kann nicht für 100-prozentige Sicherheit sorgen. So bildet Verschlüsselung beispielsweise nicht im Geringsten einen Schutz gegen Malware. Deshalb aber auf Verschlüsselung zu verzichten, wäre in etwa damit vergleichbar, dass Sie sich weigern, mit Ihrem Rheuma zum Arzt zu gehen, da Sie trotzdem an Grippe erkranken könnten. Das eine hat mit dem anderen also nichts zu tun. Die Webseitenverschlüsselung dient ausschließlich diesem Szenario: Daten, die Besucher Ihrer Website abfragen oder die sie in Ihre Websiteformulare eingeben, wandern nicht mehr im Klartext sondern verschlüsselt durchs Internet. Dritte können – aufs Wesentliche heruntergebrochen – Daten weder abfischen noch manipulieren, wenn Sie sich für eine wirksame Verschlüsselung entscheiden. Es ist empfehlenswert, dass Sie als Webmaster HTTPS und Anti-Malware-Software nutzen, um Ihre Seite abzusichern.

Und die Sache mit der Firewall? Betrachten wir zunächst, wie genau Firewalls arbeiten: Mit einer Firewall schützen Sie Ihr lokales Netzwerk, beispielsweise das unternehmensinterne Netzwerk, vor öffentlichen, unbefugten Zugriffen. Eine Firewall wird dafür genau zwischen dem lokalen und dem öffentlichen Netzwerk platziert. Oftmals ist sie Teil des Routers, kann aber auch als externe Komponente

integriert werden. Eine Firewall lässt sich also nicht mit Verschlüsselung vergleichen.

Es gibt verschiedene Möglichkeiten, eine Webseite zu verschlüsseln – wir empfehlen die Verwendung des Zusatzes Perfect Forward Secrecy (PFS). PFS sorgt dafür, dass Sitzungen Ihrer Webseitenbesucher rückwirkend nicht dechiffriert werden können. Ein sogenannter “Session-Key” (Sitzungsschlüssel) wird automatisch vernichtet, sobald der Anwender seine Sitzung beendet hat. Nun existieren bei PFS verschiedene Möglichkeiten, den Server zu konfigurieren. Möchten Sie mehr darüber erfahren, lesen Sie darüber in unserer Knowledgebase über PFS, möchten Sie sehr tief in die Materie einsteigen, haben wir auch einen Konfigurationsartikel bereitgestellt. Verlangsamte Ladezeiten sind ein weiteres Argument, das gerne herangezogen wird, um auf Verschlüsselung zu verzichten. Möglichkeiten, den PageSpeed zu optimieren, stellt Sistrix an dieser Stelle vor.

Angriffe und Schwachstellen in der Verschlüsselung

Je mehr Kenntnisse wir über Webseitenverschlüsselung erlangt haben, umso mehr Angriffsszenarien werden auch bekannt. Angriffe auf SSL-gesicherte Verbindungen häuften sich in den vergangenen Zeit: Denken Sie an Heartbleed, an ShellShock und an Poodle. Mozilla bloggt zum Poodle-Szenario, dies sei das Ende von SSL 3.0 – und tatsächlich haben neben Mozilla schon weitere Internetriesen wie Google die SSLv3-Abschaltung angekündigt. Zu unterscheiden gilt allerdings zwischen Sicherheitslücken in der Verschlüsselung selbst sowie solchen im Zertifikatesystem.

Die eingesetzten Verschlüsselungsverfahren werden in regelmäßigen Abständen geprüft. Daraus folgend kommen Sicherheitslücken wie die oben erwähnten zum Vorschein, auf die glücklicherweise umgehend reagiert wird – leider gilt dies vorrangig für die Entwickler selbst. Dass Banken und E-Mail-Provider bei Poodle etwa noch Nachholbedarf haben, zeigte Heise jüngst. Die Entwicklerseite achtet also auf regelmäßige Aktualisierungen, um Verschlüsselung sicher zu halten, auf Anwenderseite existiert die Pflicht, mitzuziehen, die leider noch oftmals vernachlässigt wird. Grundsätzlich besteht bei SSL-Verbindungen die Gefahr einer Man-in-the-middle-Attacke. Dabei schaltet sich ein Angreifer zwischen Client und Server, um so den Datenverkehr abzufangen. Abwehrmechanismen sowie weitere Informationen zu den Angriffsszenarien können Sie in diesem PDF der Hochschule Reutlingen nachlesen. Eine wirksame Gegenmaßnahme, die bereits seit September 2009 besteht, ist das HSTS-Verfahren: Die Abkürzung steht für HTTP Strict Transport Security. Moderne Browser verstehen den Standard.

Die Effizienz der Verschlüsselung hängt auch immer von den verwendeten Standards ab. Mit HSTS verwenden Sie einen zeitgemäßen Standard. Der allein reicht aber nicht: Achten Sie auch auf den Hash-

Algorithmus, der die Integrität sicherstellen soll. MD5 ist absolut veraltet und gilt als unsicher. Dasselbe Schicksal wird nun auch SHA-1 ereilen; Google und Mozilla kündigten bereits an, diesen Algorithmus zu blockieren. SHA-2 entspricht dem aktuellen Stand der Sicherheit und SHA-3 ist bereits in Entwicklung. Wenn Sie sich ein SSL-Zertifikat bestellen, achten Sie unbedingt auf die Verwendung von SHA-2 – andernfalls hat Ihr SSL-Zertifikat bald keinen sicheren Wert mehr.

Kleine FAQ-Ecke zur Verschlüsselung

“Ich blogge doch nur. Muss ich mein Blog etwa verschlüsseln?”

Sie müssen nicht, angenehmer wäre es allerdings – vor allem für Ihre Kommentatoren. Diese geben neben ihrer Meinung zu Ihren Artikeln auch ihre E-Mail-Adresse, eventuell auch die eigene Website an. Diese Informationen wandern im Klartext durchs Web, wenn Sie als Blogger auf Verschlüsselung verzichten.

“Ich verstehe die Preisgestaltung vieler Anbieter nicht.”

In der Tat: Die Preisgestaltung ist undurchsichtig. Ein guter Anbieter berät Sie telefonisch oder per E-Mail und unterstützt Sie bei der Auswahl eines passenden SSL-Zertifikats. Eine kurze Orientierungshilfe möchten wir Ihnen mitgeben:

Login-Seiten und non-eCommerce-Webseiten: domainvalidierte Einzelzertifikate schützen eine Domain, domainvalidierte Multidomainzertifikate mehrere Domains und domainvalidierte Wildcardzertifikate können alle Subdomains einer Domain verschlüsseln. Der Validierungsprozess fällt kurz aus, Ihr SSL-Zertifikat ist in der Regel in zehn Minuten einsatzbereit und die jährlichen Kosten bewegen sich um die 15 Euro. Wenn Sie sich für ein Einzelzertifikat mit einer Laufzeit von mehreren Jahren entscheiden, können Sie sich sogar länger und günstiger zurücklehnen: Für 59 Euro bestellen Sie ein SSL-Zertifikat von Comodo, einer namhaften Zertifizierungsstelle, die SHA-2 als Hash-Algorithmus bereits bedenkt und eine Laufzeit von fünf Jahren bietet.

eCommerce-Webseiten: für eine einzelne Domain wählen Sie ein organisationsvalidiertes Einzelzertifikat, bei mehreren Seiten wieder ein Multidomainzertifikat, auch Wildcardzertifikate sind möglich. Die Organisationsvalidierung ist etwas umfangreicher als die Domainvalidierung und die Kosten dieser SSL-Zertifikate sind aufgrund der intensiveren Prüfung etwas höher. Sie können mit Kosten ab 49 Euro pro Jahr rechnen; entscheiden Sie sich für längere Laufzeiten, können Sie auch hier etwas sparen.

Der Vollständigkeit halber seien auch Extended Validation-Zertifikate erwähnt, die eine sehr intensive Validierung voraussetzen. Behörden, Banken und Unternehmen, die mit der „grünen Adressleiste" bei Ihren Webseitenbesuchern mehr Vertrauen schaffen möchten, nutzen solche SSL-Zertifikate. Da diese nur für Organisationen ausgestellt werden, die in öffentlichen Registern eingetragen sind kann nicht jeder Online-Shop-Betreiber, obwohl es empfehlenswert ist, ein solches SSL-Zertifikat erwerben. Das Besondere an der Extended Validation: Browser in den neuesten Versionen sind in der Lage, zu erkennen, ob Ihr SSL-Zertifikat anhand der Extended Validation authentifiziert wurde. Ist dem so, erkennen Sie dies an der grünen Adressleiste sowie am „HTTPS" zu Beginn der Adressleiste. Das geschlossene Vorhängeschloss dient als Erkennungszeichen für eine Verschlüsselte Sitzung. Neben der Internetadresse werden der Organisationsname sowie die Zertifizierunsstelle angezeigt, was das Vertrauen Ihrer Webseitenbesucher erhöht, da diese auf einen Blick sehen, dass Ihnen der Datenschutz wichtig ist. Jeder Webseite, die mit hochsensiblen Daten agiert, etwa ein Shop, in den Kunden ihre Kreditkartendaten eingeben, ist mit einem EV-Zertifikat am besten beraten. Die Sicherheitszeichen, die ein EV-Zertifikat mit sich bringt, gelten als sofortiger Beweis Ihrer Identität und der Verschlüsselung Ihrer Website.

Um Subdomains mitabzudecken, entscheiden Sie sich für ein Multidomainzertifikat. In aller Regel sind drei Domains inklusive und bis zu 100 weitere lassen sich hinzubuchen.

"Ist die Installation eines SSL-Zertifikats schwierig?"

Keine Sorge – ein guter Anbieter lässt Sie bei der Installation Ihres SSL-Zertifikats nicht im Regen stehen. In aller Regel werden Sie durch den Support unterstützt, teilweise übernimmt dieser auch die Installation für Sie.

Fazit: Ranken Sie mit Sicherheit!

In Zeiten, in denen Sie aus allen erdenklichen Richtungen abgehört und ausspioniert werden – Hacker, Geheimdienste und Wirtschaftsspionage sind täglicher Teil medialer Berichterstattung – ist es nur sinnvoll, dass Google die Webseitenverschlüsselung als Rankingfaktor ansieht. Zahlreiche Mythen lassen das Verschlüsseln einer Website komplizierter erscheinen als sie eigentlich ist. Weder die vermeintliche Kompliziertheit noch die Kosten oder Scheinargumente wie "Verschlüsselung schützt nicht vor Malware" sollten Sie daran hindern, die Kommunikation mit Ihren Websitebesuchern abzusichern. Lassen Sie sich von Ihrem Anbieter beraten: Als Blogbetreiber greifen Sie zur einfachsten Variante, dem domainvalidierten Einzel- oder Multidomainzertifikat (je nachdem, ob Sie auch weitere Domains absichern möchten oder nicht), als Shopbetreiber sind Sie mit organisationsvalidierten SSL-Zertifikaten

richtig beraten. Unterstützung beim Installieren ist Ihnen bei guten Anbietern ebenfalls sicher. Sie profitieren nicht nur im Ranking bei Google, sondern geben Ihren Website-Besuchern auch noch die Sicherheit, dass ihre Kommunikation mit Ihnen nicht belauscht oder manipuliert werden kann.

Über den Autor:

Christian Heutger ist Geschäftsführer der PSW GROUP GmbH & Co. KG und ist seit 1998 im Bereich IT-Security tätig. Als Datenschutzauditor DSA-TÜV, IT-Security-Auditor (TÜV) und IRCA ISO 27001 Information Security Management Systems (ISMS) Auditor/Lead Auditor verfügt er über ein zertifiziertes Wissen und gilt als Experte auf diesem Gebiet. Sein Wissen über IT-Sicherheit vermittelt er zudem als Lehrbeauftragter für den DV-Bereich am Fachbereich Wirtschaft der Hochschule Fulda.