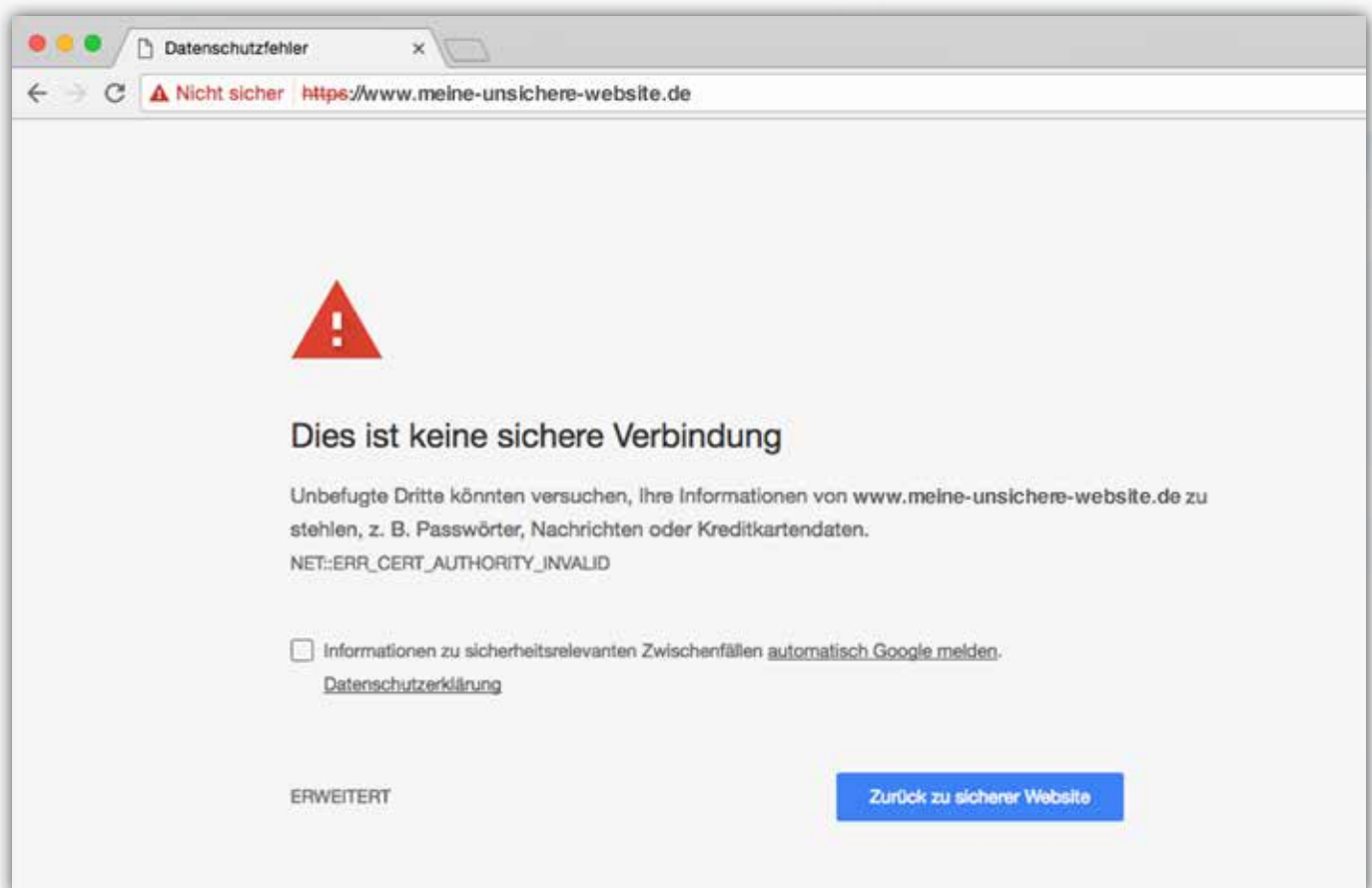


Wie sicher ist Ihre Website?

Warum eine SSL-Verschlüsselung jetzt für alle Unternehmer Pflicht ist

SSL-Verschlüsselung sollte spätestens jetzt zum Standard gehören, denn mehrere Browser warnen seit Anfang des Jahres vor nicht sicheren, also nicht verschlüsselten Seiten. Warum das auch für Ihre Webseite relevant ist und was Sie zu beachten haben, erfahren Sie in diesem Artikel.



Sie kennen sicher seit Langem die verschlüsselten Seiten Ihrer Bank oder die eines seriösen Webshops, deren URL an Stelle mit `http://` mit `https://` beginnen. Diese Seiten sind mit einem SSL-Zertifikat verschlüsselt, um sensible Daten wie Kreditkartennummern oder Bankdaten sicher zu übertragen. Man erkennt diese verschlüsselten Seiten auch am Schlosssymbol im Adressfenster, in einigen Browsern wird es zusätzlich mit dem Wort „Sicher“ und in grüner Farbe dargestellt.



Warum sollten Sie jetzt auch Ihre „normale“ Webseite verschlüsseln?

Die Rechtslage ist seit Sommer 2015 (§ 13 des Telemediengesetzes www.gesetze-im-internet.de/tmg/_13.html) dergestalt, dass Webseitenbetreiber dazu verpflichtet sind sicherzustellen, dass auch personenbezogene Daten gegen äußere Zugriffe geschützt sind.

Dies ist schon der Fall, wenn Sie lediglich ein einfaches Kontaktformular auf Ihren Seiten installiert haben, daher müssen die Daten, die dort eingegeben werden können, verschlüsselt sein. Andernfalls drohen Bußgelder.

Im Wortlaut besagt das Telemediengesetz (Auszug)

”

(...) (7) Diensteanbieter haben, soweit dies technisch möglich und wirtschaftlich zumutbar ist, im Rahmen ihrer jeweiligen Verantwortlichkeit für geschäftsmäßig angebotene Telemedien durch technische und organisatorische Vorkehrungen sicherzustellen, dass

1. kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und

2. diese

a) gegen Verletzungen des Schutzes personenbezogener Daten und

b) gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind, gesichert sind. Vorkehrungen nach Satz 1 müssen den Stand der Technik berücksichtigen. Eine Maßnahme nach Satz 1 ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens. (...)

SSL-Verschlüsselung ist neuer Rankingfaktor bei Google

Einen weiteren Grund für die sichere Verschlüsselung Ihrer Seiten gibt auch Google. Der Suchmaschinen-gigant hatte bereits 2014 in dem Blogpost mit dem eindeutigen Titel „HTTPS as a ranking signal“ angekündigt, dass https-Verschlüsselung ein Rankingfaktor sein werde. Dies ist zwar nur einer von über 200 Faktoren, die Einfluss auf das Suchmaschinenranking nehmen, aber sicherlich nicht zu vernachlässigen.

Nun warnen seit Anfang 2017 der Google-Browser Chrome und auch Firefox mit einem Info-Kästchen vor der URL vor unsicheren Seiten.

Die Verbindung zu dieser Website ist nicht sicher

Sie sollten keine vertraulichen Informationen wie Passwörter oder Kreditkartennummern auf dieser Website eingeben, da sie von Angreifern gestohlen werden könnten.

[Weitere Informationen](#)

frage bei der Zertifizierungsstelle überprüft wird. Wenn das Zertifikat gültig ist, wird eine gesicherte Verbindung zwischen Server und Browser hergestellt, und alle im weiteren Verlauf übertragenen Daten sind verschlüsselt. So wird auch sichergestellt, dass die Website tatsächlich die des Zertifikatsinhabers ist, und der Zugriff nicht zum Beispiel von einem Hacker umgeleitet wurde.

Wie Sie eine SSL-Verschlüsselung für Ihre Webseite erhalten

SSL-Zertifikate sind bei verschiedenen Anbietern wie z.B. Ihrem Provider erhältlich und müssen vom Webseiten-Betreiber erworben und installiert werden. Ein solches Zertifikat bietet eine eindeutige Identifizierung Ihrer Domain und des Hosters. Die Kosten liegen im ein- bis unteren zweistelligen Bereich pro Monat, je nach Größe der Seiten und dem gewünschten Sicherheitslevel. Die Installation können Sie beziehungsweise ein IT-versierter Mitarbeiter selber durchführen. Oder Sie beauftragen damit einen externen Dienstleister bzw. Ihre Agentur.

Was ist die SSL-Verschlüsselung?

Generell kann jede nicht verschlüsselte Datenübertragung im Internet abgefangen und manipuliert werden. Als die Übertragungsprotokolle vor etwa 30 Jahren erfunden wurden, lag der Fokus mehr auf Stabilität und Ausfallsicherheit, aber weniger auf Sicherheit beziehungsweise Authentizität der übermittelten Daten.

SSL ist die Abkürzung für „Secure Socket Layer“. Mit Layer sind bildhaft die Transportebenen gemeint, auf denen der Datenaustausch stattfindet. Wenn Sie eine Adresse im Browser eingeben, verschickt der Server, auf dem die Seite liegt, sein SSL-Zertifikat, das vom Browser durch Nach-

Worauf müssen Sie nach der Umstellung auf HTTPS achten?

Wenn das Zertifikat installiert ist, müssen alle HTTP-Links in HTTPS-Links geändert werden. Bei umfangreicheren Seiten kann das durchaus etwas länger dauern, die Verlinkung aller Seiten, Bilder oder zum Download angebotene PDF- oder Word-Dateien zu ändern und zu überprüfen. Bei der Umstellung auf HTTPS müssen zudem auch Weiterleitungen auf die neuen URLs – sogenannte Redirects – eingerichtet werden, um das jetzige Ranking nicht zu verschlechtern. Auch sollten Sie in der Google Search Console die neue HTTPS-Seite anmelden, denn für die Suchmaschinen gilt sie als neue Seite. ■



Siegbert Mattheis
Geschäftsführer
mattheis.Werbeagentur GmbH
www.mattheis-berlin.de