KEIN HTTPS?

GOOGLE CHROME WARNT VOR UNSICHERER VERBINDUNG

Google macht ernst. Ab Oktober dieses Jahres werden Webseiten, die NICHT über eine SSL-Verschlüsselung verfügen, im hauseigenen Browser Chrome als unsicher markiert. Doch zuerst einmal tief durchatmen. Was ist SSL überhaupt und wieso liegt Google dieses Thema so am Herzen?

Was ist SSL und warum brauche ich es?

SSL* ist eine Verschlüsselungstechnik, die dazu beiträgt, den Datenaustausch zwischen Webseiten-Besucher und Webseite zu verschlüsseln. Wann immer persönliche oder sensible Daten übertragen werden – z.B. über ein Formular – schützt die Verschlüsselung davor, dass Dritte diese Daten abfangen und nutzen können.

Indem Sie als Unternehmen Ihre Webseite mit einer SSL-Verschlüsselung anbieten, schützen Sie nicht nur sich selbst, sondern auch Ihre Kunden. Sie als Webseiten-Betreiber profitieren vor allem bei Anmeldeformularen von einer SSL-Verschlüsselung. Dazu gehören z.B. der Login zum Backend der Webseite oder ins Intranet. Für Webseiten-Besucher ist die Verschlüsselung vor allem beim Ausfüllen von Kontaktformularen relevant, damit persönliche Informationen wie Email-Adresse, Kundennummer oder Adresse nicht in falsche Hände geraten.

Ohne Verschlüsselung ist es Dritten grundsätzlich möglich, übermittelte Daten wie Usernamen, Passwörter oder Kundennummern abzufangen und auszulesen. Mit einer SSL-Verschlüsselung verhindern Sie zwar nicht das Abfangen von Daten, erschweren das Auslesen der Daten jedoch um ein vielfaches. Denn man müsste sagenhafte 340’282’366’920’938’463’463’374’607’431’768’211’456 Möglichkeiten durchprobieren, um eine herkömmliche 128-Bit Verschlüsselung zu knacken.

Wichtig: Eine SSL-Verschlüsselung schützt nur den Datenaustausch zwischen Webseiten-Besucher und Server und hat keinen Einfluss darauf, wie die Daten auf dem Server selbst verarbeitet oder gespeichert werden.

* SSL = Secure Sockets Layer, heute auch unter dem Begriff TSL (= Transport Layer Security) bekannt

Wie erkenne ich eine sichere Webseite?

Ob eine Webseite SSL unterstützt oder nicht, sehen Sie direkt im Browser. Chrome kennzeichnet eine sichere Seite beispielsweise mit einem grünen Schloss-Symbol. Das gleiche gilt für Firefox. In Edge wird eine funktionierende SSL-Verschlüsselung mittels grossem grauen Icon symbolisiert. Die URL einer SSL-Verschlüsselten Webseite beginnt anstatt mit dem klassischen http:// mit https:// .

Darstellung einer Seite mit SSL-Verschlüsselung

Aktuelle Darstellung einer Seite mit SSL-Verschlüsselung

Darstellung einer Seite ohne SSL-Verschlüsselung

Aktuelle Darstellung einer Seite ohne SSL-Verschlüsselung

Google und SSL

Google, als grösstem Suchmaschinenanbieter weltweit, liegt viel daran, das Internet möglichst sicher zu machen. Denn wer bei Google etwas sucht und von dort auf eine Webseite gelangt, erwartet, dass diese sicher ist. Somit hat Google ein Interesse daran, nur vertrauenswürdige Webseiten zu empfehlen. Dazu sortiert Google regelmässig Webseiten mit Malware und ähnlichen Sicherheitsproblemen aus und belohnt andererseits sichere Webseiten durch eine Verbesserung im Ranking.

Nun geht Google noch einen Schritt weiter. Ab Oktober warnt der hauseigene Browser Chrome vor Webseiten mit Formularen, die nicht verschlüsselt sind. Diese Änderung betrifft damit alle Webseiten, bei welchen Daten der Webseitenbesucher an den Server übertragen werden. Dies geschieht in der Regel über Kontaktformulare oder die Login-Funktion. Wird eine Webseite neu von Google als unsicher markiert, kann dies Ihre Besucher verunsichern, da sie das Gefühl haben, das Aufrufen Ihrer Seite sei nicht sicher. Wir möchten ja nicht den Teufel an die Wand malen, aber wie würden Sie reagieren, wenn „Nicht sicher“ vor einer URL stehen würde?

SSL-Verschlüsselung per Mausklick

Doch es gibt keinen Grund, deswegen verunsichert zu sein. Das Einrichten von SSL ist heute denkbar einfach geworden. Praktisch alle Hosting-Anbieter ermöglichen die Bestellung und Aktivierung der Verschlüsselung per Mausklick. Das beste daran: die Basis-Version ist immer kostenlos. Diese bietet die volle Verschlüsselung und damit alle Sicherheit, die Sie in der Regel brauchen.

Klassische HTML-Webseiten sind rasch umgestellt und bedürfen meistens keinerlei Anpassungen. Nutzen Sie ein CMS mit einer Datenbank, kann die Umstellung etwas komplizierter werden. Sind Sie mit WordPress unterwegs, ist aber auch das mit zwei kleinen Anpassungen erledigt.

In unserer Wissensdatenbank finden Sie eine Schritt-für-Schritt-Anleitung, wie Sie bei WordPress eine SSL-Verschlüsselung aktivieren können:

ZUR SCHRITT-FÜR-SCHRITT-ANLEITUNG

Kostenpflichtige SSL-Zertifikate

Kostenpflichtige SSL-Verschlüsselungen beinhalten zusätzlich ein Zertifikat, das auf Ihr Unternehmen ausgestellt wird. Dazu gehören meistens ein Versicherungsschutz und weitere Services. Solange Sie keinen Online Shop mit tausenden von Kunden betreiben oder hochsensible Daten über Ihre Webseite abfragen, gibt es jedoch keinen Grund, ein solches Zertifikat zu lösen.

Zusammenfassung

SSL bewahrt Sie nicht nur davor, dass Google Ihre Webseite als unsicher kennzeichnet, sondern bietet auch weitere Vorteile:

Reduktion möglicher Missbräuche,

Stärkung des Vertrauens in Ihre Webseite oder Marke und dadurch

Erhöhung der Interaktion mit Ihrem Unternehmen sowie

Verbesserung Ihres Google-Rankings und der Suchresultate und somit

Erhöhung der Anzahl Webseitenbesucher