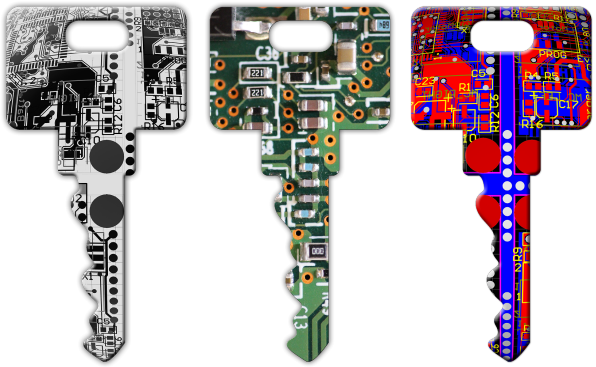
HTTPS UND SSL VERSCHLÜSSELUNG – WAS IST DAS UND WARUM IST DAS FÜR WEBSEITEN UNVERZICHTBAR?

Veröffentlicht am 7. Dezember 2017 von Jana



Was bedeutet eigentlich **HTTPS** und worin liegt der Unterschied zu **HTTP**? Und warum ist eine **SSL Verschlüsselung** so wichtig? Nicht nur für Deine eigene Website, sondern auch für Dich als Nutzer spielen beide Faktoren eine große Rolle – warum, erfährst Du hier.

Datenschutz garantieren - Du fragst auf Deiner Website personenbezogene Daten durch ein **Kontaktformular** oder ein **Bestellformular** ab? Dann solltest Du für Deine Website unbedingt ein **SSL bzw. TLS Zertifikat** nutzen. Mehr dazu erfährst Du im Folgenden.

AM ANFANG STEHEN BROWSER UND SERVER

Was passiert eigentlich, wenn man eine Internetseite aufruft? Technisch gesehen ist das eine riesige Abfolge von Schritten, die wir euch an dieser Stelle ersparen wollen. Wichtig ist aber, dass Dein Browser bei einem Webseitenaufruf eine Verbindung mit dem entsprechenden Webserver herstellt und **Daten** anfordert. Dabei bildet ein **Protokoll** eine gemeinsame Sprache, um die Verständigung sicherzustellen. Dabei können zwei verschiedene Protokolle zum Einsatz kommen:

HTTP ODER HTTPS

HTTP steht für HyperText Transfer Protocol und wird verwendet, damit ein Browser auf eine Website zugreifen kann.

Client und **Server** tauschen Nachrichten bzw. Informationen über das HyperText Transfer Protocol aus: Dazu sendet der Client eine **Anfrage (Request)** an den Server, dieser gibt wiederum die **Antwort (Response)** an den Client zurück. Diese Nachrichten bestehen aus zwei Teilen: dem Header (Nachrichtenkopf), der Informationen über verwendete Kodierungen und Inhaltstyp enthält, und dem Body (Nachrichtenrumpf), der wiederum Nutzdaten beinhaltet.

Was ist ein Client?
Ein Client (dt. Kunde) ist in der IT ein Computerprogramm. Ein typischer Client ist zum Beispiel ein **Webbrowser**. Damit Du Dir eine Website im Internet anzeigen lassen kannst, muss der Browser Kontakt zum **Webserver** aufnehmen. Und wie oben beschrieben, Nachrichten bzw. **Informationen** austauschen, damit der Browser die Homepage anzeigen kann.

Bei dem HyperText Transfer Protocol handelt es sich um ein **zustandsloses Protokoll**: mehrere unterschiedliche Anfragen werden dabei als voneinander unabhängige Transaktionen behandelt. Klingt erst mal solide, jedoch birgt HTTP Nachteile: jeder könnte mitlesen. Was genau bedeutet das? Alle übermittelten Daten zwischen Browser und Server werden online über eine Leitung geschickt. Jeder, der Zugriff auf dem Weg der Daten bekommt, kann sie **mitlesen und sogar manipulieren** – und das ohne, dass man es selbst bemerkt. Welche **Folgen** das mit sich bringen kann, wird später noch angesprochen.

HTTP Verbindungen sind daher unsicher und sollten durch **zusätzliche Sicherheitsmaßnahmen** ergänzt werden.

An dieser Stelle kommt **HTTPS** ins Spiel: HTTPS steht für HyperText Transfer Protocol Secure und ist ein **abhörsicheres Protokoll**, das Daten zwischen Browser und Server in beide Richtungen **verschlüsselt** überträgt.

Zuerst etablierte sich HTTPS im Online-Shopping, bei dem viele Anbieter die Kaufabwicklung absicherten. Darauf folgten E-Mail Provider und soziale Netzwerke, die ihre Verbindungen mit HTTPS schützten.

Dabei arbeiten beide Seiten mit einem nur für sie erkennbaren **Schlüssel**, der durch die vorher ausgetauschten Daten auf eine komplexe Weise berechnet wird. Die Dateninformationen zur

Generierung der Schlüssel sind bei einer Ausspionierung einsehbar, lassen aber keine Hinweise auf den Schlüssel selbst zu. Im nächsten Schritt wird ein weiterer Schlüssel ausgetauscht, mit dem die zu sendenden Daten verschlüsselt werden.

MERKE: Das textbasierte HyperText Transfer Protocol ist nicht ausreichend um Deine Website effektiv gegen Datenklau im **Internet** zu schützen. Setze auf HyperText Transfer Protocol Secure, das durch **Zertifikate** - ein SSL (Secure Socket Layer) bzw. ein TLS (Transport Layer Security) Zertifikat - die Sicherheit Deiner Website erhöht. Aber dazu gleich mehr.

WARUM EINE SICHERE VERBINDUNG?

Befinden sich Nutzer auf einer HTTP Seite, kann das **Folgen** mit sich ziehen. Vor allem dann, wenn es um **personenbezogene Daten** geht, ist eine sichere Verbindung **verpflichtend**. Gerade für folgende beispielhafte **sensible Daten** spielt das eine große Rolle:

- Online-Banking oder Zahlungsabwicklungen über PayPal
- E-Mails mit sensiblem Inhalt
- Übertragung von Cloud-Daten, wie zum Beispiel Dropbox
- Nutzung von sozialen Netzwerken
- Registrierung oder Anmeldung auf Websites über Benutzername und Passwort

Bei allen Anwendungen, bei denen Passwörter oder PINs und TANs verwendet werden, ist eine HTTPS Verbindung zwingend notwendig. Kommen diese Daten in die falschen Hände, kann das fatale Auswirkungen haben. Vor allem wenn in **offenen Netzwerken** gesurft wird, muss verstärkt aufgepasst werden. Hier hat der Hacker die Chance, einen vom ihm gesteuerten WLAN-Zugang mit einem seriösen Namen zu versehen und geöffnet zu lassen. Hier fungiert er als so genannter Man-In-The-Middle und kann Datenverkehre mitlesen und manipulieren.

Tipp: Stelle in Deinem Smartphone ein, dass es sich nicht automatisch mit offenen **WLAN Netzwerken** verbindet. Achte auch darauf, in welche Hotspots Du Dich einwählst. Wird Dir zum Beispiel ein kostenloser Hotspot von einer Restaurantkette angezeigt und Du findest in Deiner unmittelbaren Nähe keine entsprechende Filiale, solltest Du misstrauisch werden.

SCHLÜSSEL BENÖTIGEN EIN ZERTIFIKAT

HTTPS verschlüsselt nicht nur Daten, sondern prüft auch die **Echtheit des Kommunikationspartners**. Dafür wird von unabhängigen Zertifikationsstellen ein **digitales Zertifikat** ausgestellt. Mit diesem kann dann belegt werden, dass es sich tatsächlich um die Domain handelt, die der Nutzer kontaktieren will.

Heutzutage, in denen **Datensicherheit** im Internet immer größer geschrieben wird, prüfen viele Browser diese Zertifikate automatisch. Wurden Zertifikate von unseriösen Zertifizierungsstellen ausgestellt oder ist ein Zertifikat abgelaufen oder unvollständig, wird dem Nutzer eine **Warnung** ausgegeben. Browser haben hier eine Liste von vertrauenswürdigen Zertifikaten, die regelmäßig aktualisiert wird.

SSL VERSCHLÜSSELUNG

Was ein Protokoll ist und wofür es benötigt wird, wurde schon angesprochen. Um aus einer HTTP Verbindung nun eine HTTPS Verbindung zu machen, wird eine **SSL Verschlüsselung** verwendet. SSL steht für Secure Socket Layer und wurde von der Netscape Communications Corporation entwickelt. Der Nachfolger von SSL ist **TLS**, was für Transport Layer Security steht – im allgemeinen Sprachgebrauch wird allerdings immer noch von SSL gesprochen. Mit Layer sind in beiden Begriffen die Transportebenen gemeint, auf denen der Datenaustausch stattfindet. Da HTTPS und SSL/TLS immer im Zusammenhang stehen, spricht man daher auch von HTTP via SSL/TLS.

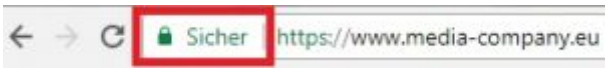
Bei den eben erwähnten Zertifikaten handelt es sich dabei immer um SSL Zertifikate. Nur mit einer SSL Verschlüsselung und richtigem Zertifikat kann also eine sichere Verbindung zwischen Browser und Server aufgebaut werden.

WICHTIG: Mit dem Inkrafttreten der DSGVO – der europäischen Datenschutzgrundverordnung – am 25. Mai 2018 müssen **personenbezogene Daten** im Internet verschlüsselt werden. Jede Website, die persönliche Daten von Nutzern zum Beispiel über ein **Kontaktformular** oder **Bestellformular** abfragt, muss über eine sichere SSL Verbindung verfügen. Du solltest also spätestens jetzt aktiv werden und dafür sorgen, dass Deine Website mit einem SSL Zertifikat ausgestattet ist. Denn: Ohne ein SSL Zertifikat besteht eine **Sicherheitslücke** und als Verantwortlicher bzw. Inhaber einer Website haftest Du für eventuellen Datenklau bzw. Datenmissbrauch.

Du möchtest mehr über die DSGVO und wie sich Unternehmen vorbereiten müssen erfahren? Dann lies unseren DSGVO Blogbeitrag.

WIE ERKENNE ICH SICHERE SEITEN?

Je nach Browser gibt es verschiedene Darstellungen. In den meisten Fällen hat sich jedoch das **Schloss-Symbol** bewährt, hinter dem mit einer grünen Schrift auf eine sichere Verbindung hingewiesen wird.



HTTPS/SSL Verschlüsselung

HTTPS kann im schlimmsten Fall allerdings auch vorgetäuscht sein. Mit überdurchschnittlichen Programmiertechniken können Teile des Browser Fensters nachgebildet werden. Zum Beispiel kann eine Login-Seite durch eine gefälschte Seite ausgetauscht werden. Ist diese gut gemacht, lässt sich die Fälschung vom Original für den normalen Nutzer nicht unterscheiden. So werden sensible Daten direkt an den Hacker verschickt.

Will man sich das **Zertifikat der Domain** anschauen, so kann das mit einem Klick auf das Schloss Symbol aufgerufen werden. Falls Dein Browser Dich nicht schon gewarnt hat, kannst Du dann einsehen, ob das Zertifikat gültig ist, von welcher Stelle es ausgestellt wurde und wer der tatsächliche Kommunikationspartner ist bzw. ob es sich um den handelt, den Du auch erreichen willst. Wird zum Beispiel der Firmenname nicht angezeigt, wie in dem folgenden Beispiel, solltest Du misstrauisch werden.



SSL Zertifikat

WORAUF NUTZER ACHTEN SOLLTEN

In den letzten Jahren kam es zu Angriffen auf HTTPS – bekannt ist hier vor allem der sogenannte **„Heartbleed-Bug“**. Dabei handelt es sich um einen Programmfehler innerhalb OpenSSL, der sensible Daten von Verbindungen zwischen Browsern und Servern mitlesen konnte. Dieser ist zwar mittlerweile behoben, jedoch waren dafür **Updates** nötig. Als Nutzer solltest Du daher Deine Browser regelmäßig aktualisieren und gegebene Warnungen nicht einfach ignorieren.

Gerade in der heutigen digitalen Zeit wird das Thema **Datenschutz** immer wichtiger. Achte daher darauf, auf welchen Seiten Du surfst und welche Daten Du auf welchen Plattformen preisgibst. Vor allem bei privaten Daten ist ein **umsichtiges Surfverhalten** wichtig – nur so kannst Du Dich vor Hackerangriffen und damit Angriffen auf Deine Privatsphäre schützen.

Warum alle Websites HTTPS brauchen

Da vielen Nutzern genau dieser Datenschutz immer wichtiger wird, sollten alle Website Anbieter auf eine HTTPS und somit SSL Verschlüsselung setzen. Vor allem dann, wenn Du ein Kontaktformular anbietest, haben Nutzer ein besseres Gefühl bei dem Absenden ihrer personenbezogenen Daten.

Seit August 2017 gibt Goolge im Chrome Browser darüber hinaus **Sicherheitswarnungen** aus, wenn eine Website noch mit HTTP abrufbar ist. Das gilt sowohl bei Seiten, auf denen eine Dateneingabe möglich ist, als auch die Nutzung einer Kommentarfunktion und Newsletter-Anmeldung. Der langfristige Plan von Google sieht vor, dass alle HTTP Webseiten als „nicht sicher" eingestuft und dem Nutzer als solches angezeigt werden. Nach neuesten Informationen kündigt Google in einem Blogbeitrag an, dass mit Chrome 68 genau dieses Update kommt - schon im Juli diesen Jahres. Webseiten-Betreiber sollten also unbedingt auf HTTPS umsteigen, um keinen **Traffic** auf ihrer Seite zu verlieren und potenzielle Kunden abzuschrecken. Noch deutlicher wird das, wenn Du Dir folgendes Szenario vorstellst: Ein User besucht Deine Website, um sich über Deine Leistungen zu informieren und sogar das **Kontaktformular** für eine Kontaktaufnahme nutzen möchte. Er klickt also Deine Seite an – und sieht, wenn er Chrome als Browser benutzt, als erstes eine **Warnung von Google**. An dieser Stelle wird er darauf hingewiesen, dass eine **Verbindung beim Surfen nicht sicher** ist und gefragt, ob er die Seite trotzdem besuchen möchte. Dieses Szenario stellt nicht nur eine erste **Hürde** für einen potenziellen Kunden dar – je nach Branche und Konkurrenz wird er die Seite bereits hier schon verlassen – sondern gibt ihm auch ein ungutes Gefühl.

Doch nicht nur das: Google belohnt eine HTTPS Verbindung, indem er **Deine Website im Ranking steigen lässt**. Auch Google ist bemüht, das Internet sicherer zu machen und rankt so SSL verschlüsselte Seiten besser.

MERKE: Durch eine sichere Internetverbindung haben Nutzer mehr **Vertrauen** in Deine Website und in den dort verbreiteten Content. Sie fühlen sich sicherer und wissen, dass ihre Daten geschützt sind. Ebenfalls **Google** belohnt SSL zertifizierte Websites bzw. eine sichere HTTPS Verbindung: Im Ranking bevorzugt Google Websites mit SSL Zertifikat. Neben vielen weiteren **SEO Maßnahmen**, ist die Einbindung eines Sicherheitszertifikats also eine effektive Möglichkeit, die eigene Website zu pushen und Konkurrenten abzuhängen.

Betreibst Du eine Website, die keine https verschlüsselte Domain hat? Dann wird es höchste Zeit –

wir von der Media Company helfen Dir gern. Wir sorgen nicht nur mit einer sicheren Website für ein besseres Google Ranking, sondern auch durch gezielte Online-Marketing Maßnahmen. Kontaktiere uns jetzt – wir freuen uns auf Dein Anliegen!

Kontakt aufnehmen