Warum HTTPS verwenden?

Browser markieren Websites ohne HTTPS als „nicht sicher", einer von vielen Gründen, eine Website zu sichern.

Lernziele

Nach Lektüre dieses Artikels können Sie Folgendes:

- Wie hat sich HTTP-Traffic verändert?
- Was sind die Mythen und Wahrheiten über HTTP?
- Die Gründe für die Verwendung von HTTPS verstehen

ÄHNLICHE INHALTE

HTTPS
Was ist SSL?
Was ist ein SSL-Zertifikat?
SSL-Handshake
Keyless SSL

Link zum Artikel kopieren f0r

Was ist der Unterschied zwischen HTTP und HTTPS?

HTTPS ist HTTP mit TLS-Verschlüsselung. HTTPS verwendet TLS (SSL), um normale HTTP-Anfragen und -Antworten zu verschlüsseln und sie auf diese Weise sicherer zu machen. Eine Website, die HTTPS verwendet, hat https:// am Anfang ihrer URL anstelle von http://, wie z. B. https://www.cloudflare.com.

Warum sollten Websites also HTTPS verwenden?

Grund Nr. 1: Websites, die HTTPS verwenden, wirken auf Benutzer vertrauenswürdiger.

Eine Website, die HTTPS verwendet, ist wie ein Restaurant, das beweisen kann, dass es Hygienevorschriften erfüllt: Potenzielle Kunden können darauf vertrauen, dass sie sich beim Essen keinen großen Risiken aussetzen. Und heutzutage ist die Verwendung von HTTP im Wesentlichen so, als wäre das Restaurant durch die Überprüfung durchgefallen, es gibt keine Garantie dafür, dass einem Kunden nichts Schreckliches passiert.

HTTPS verwendet das SSL/TLS-Protokoll, um die Kommunikation zu verschlüsseln, sodass Angreifer keine Daten stehlen können. SSL/TLS bestätigt außerdem, dass ein Website-Server der ist, der er vorgibt zu sein, und verhindert so Identitätsdiebstahl. Dies stoppt mehrere Arten von Cyber-Angriffen (genau wie die Hygienevorschriften Krankheiten verhindern).

Auch wenn einige Benutzer die Vorteile von SSL/TLS nicht kennen, sorgen moderne Browser dafür, dass sie sich dennoch der Vertrauenswürdigkeit einer Website bewusst sind.

Chrome und andere Browser markieren alle HTTP-Websites als „nicht sicher".

Google hat über mehrere Jahre hinweg nach und nach Schritte unternommen, um Websites zur Integration von HTTPS zu bewegen. Google verwendet HTTPS auch als Qualitätsfaktor für die Rückgabe von Suchergebnissen. Je sicherer die Website ist, desto unwahrscheinlicher ist es, dass der Besucher einen Fehler macht, indem er auf den von Google bereitgestellten Link klickt.

Mit der Veröffentlichung von Chrome 68 im Juli 2018 wurde der gesamte ungesicherte HTTP-Traffic in der URL-Leiste als „nicht sicher" gekennzeichnet. Diese Benachrichtigung wird für alle Websites ohne gültiges SSL-Zertifikat angezeigt. Andere Browser sind diesem Beispiel gefolgt.

Grund Nr. 2: HTTPS ist sowohl für Benutzer als auch für Websitebesitzer sicherer.

Mit HTTPS werden Daten während der Übertragung in beide Richtungen verschlüsselt: zum und vom Ursprungsserver. Das Protokoll schützt die Kommunikation, sodass böswillige Parteien nicht sehen können, welche Daten gesendet werden. Infolgedessen können Benutzernamen und Passwörter während der Übertragung nicht gestohlen werden, nachdem Benutzer sie in ein Formular eingegeben haben. Wenn Websites oder Webanwendungen vertrauliche oder personenbezogene Daten an Benutzer senden müssen (z. B. Bankkontoinformationen), schützt die Verschlüsselung auch diese Daten.

Grund Nr. 3: HTTPS authentifiziert Websites.

Benutzer von Ridesharing-Apps wie Uber und Lyft müssen nicht auf gut Glück in ein unbekanntes Auto steigen, nur weil der Fahrer sagt, dass er gekommen ist, um sie abzuholen. Stattdessen teilen ihnen die Apps Informationen über den Fahrer mit, wie seinen Namen und sein Foto, welche Art von Auto er fährt und das Kennzeichen. Der Benutzer kann diese Dinge überprüfen und sicher sein, dass er in das richtige Auto einsteigt, obwohl jedes Ridesharing-Auto anders ist und er den Fahrer noch nie gesehen hat.

Wenn ein Benutzer zu einer Website navigiert, stellt er in Wirklichkeit eine Verbindung zu weit entfernten Computern her, von denen er nichts weiß und die von Personen verwaltet werden, die er noch nie gesehen hat. Ein SSL-Zertifikat, das HTTPS aktiviert, entspricht den Fahrerinformationen in der Ridesharing-App. Es ist eine externe Überprüfung durch einen vertrauenswürdigen Dritten, der garantiert, dass ein Webserver der ist, der er vorgibt zu sein.

Dies verhindert Angriffe, bei denen ein Angreifer dem Benutzer eine gefälschte Website bereitstellt, sodass Benutzer glauben, dass sie sich auf der Website befinden, die sie erreichen möchten, wenn sie sich tatsächlich auf einer gefälschten Version befinden. Die HTTPS-Authentifizierung trägt auch wesentlich dazu bei, dass eine Unternehmenswebsite legitim erscheint. Dies beeinflusst wiederum die Einstellung der Benutzer gegenüber dem Unternehmen selbst. (Benutzer können überprüfen, ob eine Website HTTPS ordnungsgemäß verwendet, indem sie die Website im Cloudflare Diagnostic Center testen.)

HTTPS-Mythen

Viele Websites haben HTTPS nur langsam eingeführt. Um herauszufinden, warum dies der Fall ist, müssen wir in die Geschichte blicken.

Als die Einführung von HTTPS begann, war die ordnungsgemäße Implementierung schwierig, langsam und teuer. Man konnte es nur schwer ordnungsgemäß implementieren, es hat Internetanfragen verlangsamt und die Kosten in die Höhe getrieben, da teure Zertifikatdienste erforderlich waren. Keines dieser Hindernisse ist heute noch aktuell. Aber viele Websitebesitzer haben nach wie vor Angst, den Wechsel zu mehr Sicherheit zu wagen. Schauen wir uns einige der Mythen über HTTPS an.

„Ich verarbeite auf meiner Website keine sensiblen Informationen, daher benötige ich kein HTTPS"

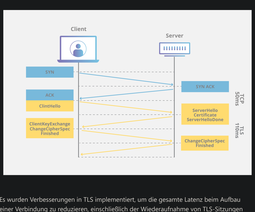
Viele Websites implementieren keine Sicherheitsvorkehrungen, weil sie denken, dass es für ihre Zwecke übertrieben ist. Wenn Sie nicht mit sensiblen Daten arbeiten, was macht Snooping dann so schlimm? Es gibt einige Gründe, warum dies eine zu vereinfachte Sichtweise auf Websicherheit ist. Beispielsweise fügen einige Internetprovider tatsächlich Werbung in von HTTP bereitgestellte Websites ein. Diese Anzeigen können mit dem Inhalt der Website übereinstimmen oder nicht und können möglicherweise anstößig sein, abgesehen von der Tatsache, dass der Website-Anbieter keinen kreativen Input beiträgt oder vom Umsatz profitiert. Auf einer gesicherten Website sind diese injizierten Anzeigen nicht mehr möglich.

Moderne Webbrowser beschränken jetzt die Funktionalität für unsichere Websites. Wichtige Features, die die Qualität der Website verbessern, erfordern jetzt HTTPS. Geolokation, Push-Benachrichtigungen und die Service-Workers, die zum Ausführen von progressiven Webanwendungen (PWAs) erforderlich sind, brauchen erhöhte Sicherheitsstufen. Das ist sinnvoll, weil Daten wie der Standort eines Benutzers vertraulich sind und für schädliche Zwecke verwendet werden können.

„Ich möchte die Performance meiner Website nicht durch erhöhte Ladezeiten beeinträchtigen."

Performance ist ein wichtiger Faktor sowohl für die Nutzererfahrung als auch für die Art und Weise, wie Google seine Suchergebnisse anzeigt. Verständlicherweise muss man die Erhöhung der Latenz ernst nehmen. Glücklicherweise hat sich HTTPS im Laufe der Zeit verbessert, um den für den Aufbau einer verschlüsselten Verbindung erforderlichen Performanceaufwand zu verringern.

Wenn eine HTTP-Verbindung hergestellt wird, muss die Verbindung zwischen dem Client, der die Webseite anfordert, und dem Server mehrmals hin- und herwandern. Abgesehen von der normalen Latenz, die mit einem TCP-Handshake verbunden ist (unten blau dargestellt), muss ein zusätzlicher TLS/SSL-Handshake (gelb dargestellt) stattfinden, um HTTPS verwenden zu können.



Es wurden Verbesserungen in TLS implementiert, um die gesamte Latenz beim Aufbau einer Verbindung zu reduzieren, einschließlich der Wiederaufnahme von TLS-Sitzungen und des TLS-Fehlstarts.

Indem TLS-Sitzungen wieder aufgenommen werden, kann ein Server eine Verbindung länger am Leben erhalten, indem dieselbe Sitzung für zusätzliche Anfragen fortgesetzt wird. Wenn Sie die Verbindung am Leben erhalten, sparen Sie Zeit beim Neuverhandeln der Verbindung, wenn der Client einen nicht zwischengespeicherten Ursprungsabruf benötigt, und reduzieren so die gesamte RTT um 50 %.

Eine weitere Geschwindigkeitsverbesserung beim Erstellen verschlüsselter Kanäle, besteht darin, einen Prozess namens TLS-Fehlstart zu implementieren, der die Latenz verringert, indem die verschlüsselten Daten gesendet werden, bevor der Client die Authentifizierung abgeschlossen hat. Wenn Sie mehr erfahren möchten, lesen Sie, wie TLS/SSL auf einem CDN funktioniert.

Und schließlich bietet TLS 1.3 sogar noch deutlichere Performance-Verbesserungen. TLS-Handshakes in TLS 1.3 erfordern nur noch einen Round Trip – und wenn der Client zuvor eine Verbindung hergestellt hat, sogar keinen Round Trip. Wenn Sie sich bei Cloudflare anmelden, können Sie ganz einfach TLS 1.3 für eine Website aktivieren.

„Die Implementierung von HTTPS ist mir zu teuer"

Es gab Zeiten, da traf dies vielleicht zu, aber jetzt sind die Kosten kein Problem mehr: Cloudflare bietet Websites die Möglichkeit, die Übertragung kostenlos zu verschlüsseln. Wir waren die ersten, die SSL kostenlos zur Verfügung stellten, und wir tun dies auch weiterhin. Indem wir die Internetsicherheit insgesamt verbessern, können wir dazu beitragen, das Internet sicherer und schneller zu machen.

„Ich werde meinen Platz im Suchranking verlieren, während ich meine Website auf HTTPS migriere"

Mit der Website-Migration sind Risiken verbunden, und bei unsachgemäßer Ausführung ist eine negative SEO-Auswirkung tatsächlich möglich. Mögliche Fallstricke sind Ausfallzeiten der Website, nicht gezeichnete Webseiten und die Bestrafung für die Dublizierung von Inhalten, wenn zwei Kopien der Website gleichzeitig vorhanden sind. Wenn Websites allerdings den Best Practices folgen, können sie sicher auf HTTPS migriert werden.

Zwei der wichtigsten Migrationspraktiken sind:

1) Verwenden von 301 Weiterleitungen und 2) richtige Platzierung Canonical Tags. Durch die Verwendung von Server 301-Weiterleitungen auf der HTTP-Site, um auf die HTTPS-Version zu verweisen, weist eine Website Google an, für alle Such- und Indizierungszwecke an den neuen Speicherort zu wechseln. Durch das Platzieren von Canonical Tags allein auf der HTTPS-Site wissen Crawler wie Googlebot, dass der neue sichere Inhalt in Zukunft als kanonisch betrachtet werden sollte.

Wenn Sie eine große Anzahl von Seiten haben und befürchten, dass das erneute Crawlen zu lange dauert, wenden Sie sich an Google und teilen Sie Google mit, wie viel Verkehr Sie über Ihre Website zu schalten bereit sind. Die Netzwerktechniker erhöhen dann die Crawl-Rate, um Ihre Website schnell zu analysieren und zu indizieren.