2019

SSL-Verschlüsslung

KOMPETENZNACHWEIS

NURIA ANAYA, ADRIANA ARTEAGA,
ANDREAS NYDEGGER, KEVIN SCHLEUNIGER

WRH | [Firmenadresse]

Inhalt

Einleitung

Wenn man im Internet eine Webadresse wie z.B. http://google.ch eingibt, wird im Hintergrund ein normales TCP-Paket an den Webserver über Port 80 gesendet. Diese TCP-Pakete können wir aber mit Programmen relativ einfach abfangen und auslesen, da sie nicht verschlüsselt sindBeim Online-E-Jedoch wenn man http://google.ch in unserem Browser eingibt fällt sofort auf, dass oben ein Grünes Schloss erscheint und die Adresse nebenbei hat zu https://google.ch ändert:

Somit weiss man, dass dieses Paket verschlüsselt ist. Die Verschlüsselung dieser Daten werden mit TLS (SSL) gemacht.

SSL-Verschlüsselung

SSL ist die Abkürzung für Secure Socket Layer und ist ein Synonym für die Verschlüsslung von Online-Datenströmen geworden. Dabei wird das originale SSL-Format nicht mehr verwendet – es wurde durch den neueren uns sicheren TLS (Transport Layer Security) Standard ersetzt.

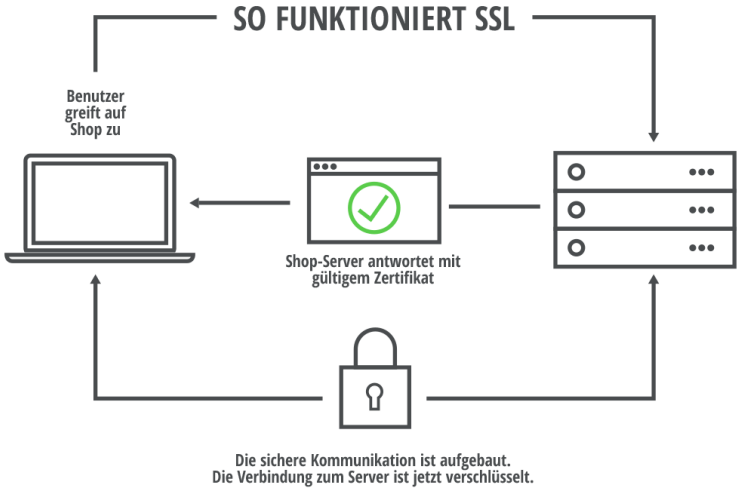
HTTP/HTTPS

Eine gesicherte Verbindung erkennt man über das HTTPS-Protokoll. Dies ist, wie auch das HTTP-Protokoll, ein Kommunikationsprotokoll zur Datenübertragung im Internet. Der Unterschied zwischen HTTPS und HTTP besteht in der verschlüsselten und abhörsicheren Übertragung der Daten mittels TLS.

Merke: HTTP**S** = HTTP +SSL/TL**S**

Wie funktioniert die SSL-Verschlüsselung?

Um eine verschlüsselte Verbindung zum Browser aufzubauen, muss der Browser wissen, ob der Server auch zu der Domain gehört, für die er sich ausgibt. Hierzu werden SSL-Zertifikate genutzt.



SSL Zertifikat

Das SSL-Zertifikat ist eine Methode, um die Authentizität einer Webseite zu verifizieren. Für das muss die Webseite ein Zertifikat bei einer anerkannten Zertifikatstelle beantragen.

Nach der Verifizierung der Domain wird bei der Certification Authorities (CA, Zertifizierungsstellen) auch der öffentliche Schlüssel hinterlegt. Mit diesem kryptographischen Schlüssel werden dann die Nachrichten verschleiert. Um die Nachricht wieder in den Ursprungszustand zu verändern, wird ein weiterer Schlüssel benötigt, der private Schlüssel. Dieser private Schlüssel ist einzig auf dem verifizierten Server fest installiert und kann die Nachrichten entschlüsseln. Das wichtige hierbei ist,

dass eine Nachricht, die mit einem öffentlichen Schlüssel enkodiert wurde, nicht mit dem gleichen öffentlichen Schlüssel dekodiert werden kann. Die Anleitung, wie eine Nachricht zu verschlüsseln ist, kann also frei verfügbar gemacht werden, während die einzige Möglichkeit die verschlüsselte Nachricht wieder zu dekodieren hinter Schloss und Riegel gehalten wird.

Welche verschiedenen SSL-Zertifikate gibt es?

- Domain Validierung (Domain Validation)
- Organisationalen Validierung (Organizational Validation)
- Erweiterten Validierung (Extended Validation)

CASC und SSL Einbindung

Nachdem man sich für eine SSL-Zertifikatsform entschieden hat, kann man dieses von einem CA Security Council (CASC) autorisierten Anbieter erwerben.
Gängige Anbieter sind z.B.:

- GlobalSign
- Geo Trust
- Symantec
- AlphaSSL
- RapidSSL
- Thawte

Die Anleitung zur Implementation wird meistens vom Zertifikats-Anbieter mitgeliefert.

Ein Beispiel solch einer Implementation von de.ryte.com wäre:

1. Installiere das SSL-Zertifikat auf Deinem Server. Wenn Du keinen dedizierten Server verwendest, bieten manche Webhoster mit wenigen Klicks eine SSL-Lösung an. Wie das SSL-Zertifikat implementiert wird, hängt von Deinem Servertyp ab. Eine gute Übersicht über die Installation des SSL-Zertifikats auf verschiedenen Servern wie Apache oder Exchange findest Du hier.

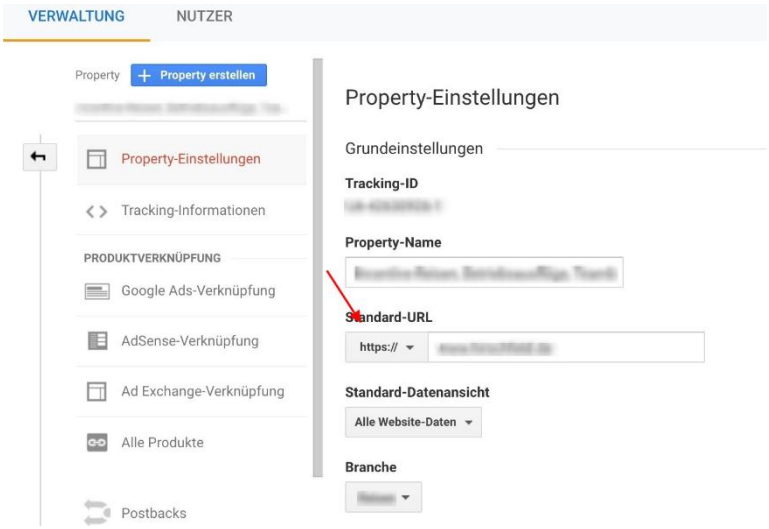
2. Wähle danach aus, welche Seiten, Subdomains oder Domains mit dem Zertifikat geschützt werden sollen.

3. Rufe Deine Seiten mit verschiedenen Browsern auf. Lass Dir anzeigen, ob noch Elemente ohne SSL-Verschlüsselung geladen werden. Mit einem SSL Checker wie von sslshopper.com kannst Du kostenlos prüfen, ob Deine SSL-Verbindung korrekt implementiert ist.

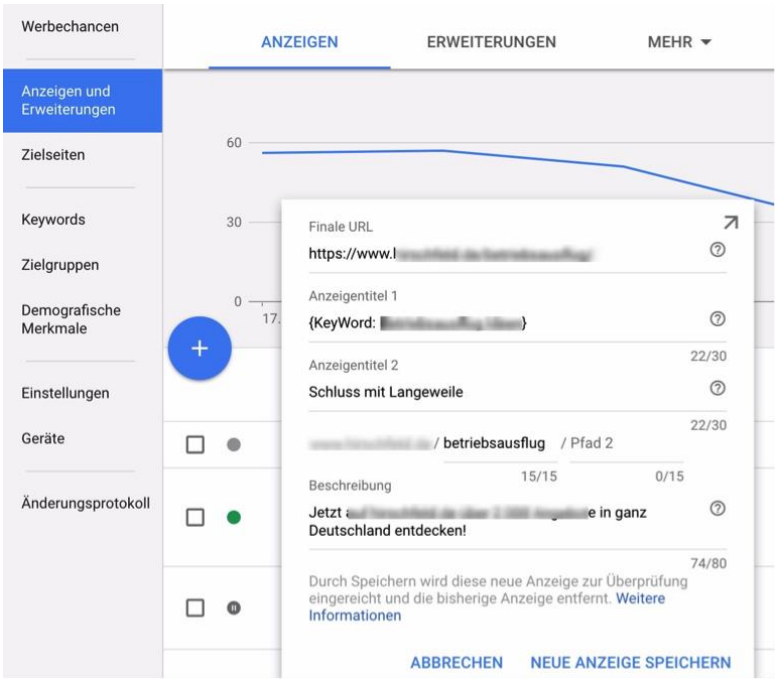
SSL-Implementation: Checkliste dannach

Zum Schluss sollte man sich noch auf folgende Sechs Punkte achten:

1. Eine 301-Weiterleitung von Deiner Webseite mit http auf https einzurichten um eine doppelte indexierung beider Versionen bei Google zu verhindern.
2. Deine https-Domain in der Google Search Console hinterlegen damit Google Daten wie Klicks oder Fehler zu deiner Webseite korrekt ermittelt
3. Die https-Seite in deinen Webanalyse-Tools zu hinterlegen für korrektes Tracking bei z.B. Google Analytics oder anderen Webanalysetools



4. Interne Links anpassen und https davorsetzten, damit die Verbindungen sicher werden
5. Adwords oder andere Werbeprogramme anpassen und die hinterlegten Links zur Domain korrigieren



6. Die https-Domain auch bei Sozialen Netzwerkprofilen wie Facebook oder Twitter hinterlegen

Quellen

https://www.sistrix.de/frag-sistrix/google-algorithmus-aenderungen/https-ranking-faktor-update/was-ist-eine-ssl-verschluesselung-und-welche-rolle-spielt-diese-bei-seo/#Wie_funktioniert_die_SSL-Verschluesselung

https://de.ryte.com/magazine/ssl-zertifikat-einrichten-schritt-fuer-schritt-zur-verschluesselten-website