Die ASW publiziert in loser Folge Beiträge von Inter-Mitgliedern zu aktuellen Themen. Derzeit ist es ein Beitrag unseres Hosters Webstyle aus Burgdorf zum Thema TLS-Zertifikate.

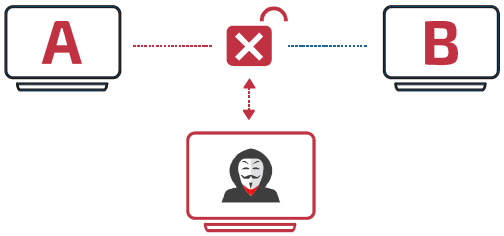
---

webstyle

Der Velo-Kurier war ziemlich baff. Soeben hatte ihm jemand eine 1'000 Franken-Note in die Hand gedrückt. Er musste weder die Entgegennahme dieses Betrages quittieren noch wurde er aufgefordert, dasselbe vom Empfänger einzufordern.
Der Kurier hätte die echte 1'000 Franken-Note gegen zwei gefälschte 500-er austauschen können. Das wäre wohl für immer und ewig sein Geheimnis geblieben.

Exakt so funktioniert jedoch die **unverschlüsselte** Übertragung von Websites im Internet. Die Gewissheit, dass der Empfänger **im Original** erhält, was der Absender in Auftrag gegeben hat, fehlt.

Was bei einer Hobby-Website nicht ganz so kritisch scheint, sieht bei Sites mit kommerziellen Ansprüchen schon ganz anders aus. Der Absender möchte Gewissheit haben, dass die Besucher seiner Website auf ihren Displays angezeigt bekommen, was er ins Netz gestellt hat. Und er möchte sicher sein, dass die ein- und ausgehende Kommunikation über seine Website nicht manipuliert werden kann, zum Beispiel von (Geld)Fälschern.



Um beim obigen Beispiel zu bleiben: Der Absender der 1000 Franken müsste **sowohl** die Entgegennahme durch den Velo-Kurier **als auch** die Auslieferung der 1'000 Franken-Note beim Empfänger quittieren lassen. Der Empfänger müsste ihm **darüber hinaus direkt** die Seriennummer der erhaltenen Banknote bestätigen. Nur so ist sichergestellt, dass «Im Original ausgeliefert und im Original angekommen» tatsächlich stattgefunden hat. Genau nach diesem Prinzip funktioniert die **verschlüsselte** Übertragung von Dateien im Internet.

Für die abgesicherte Übertragung von Dateien im Internet wurde das TLS-Protokoll (Transport Layer Security) erfunden. Es ist die Nachfolgerin des SSL-Protokolls (Secure Sockets Layer).

Die verschlüsselte Übertragung von Dateien zwischen Absender und Empfänger ist erkennbar an einem «s», das der Protokoll-Bezeichnung angefügt wird. Dieses «s» steht für «Secure».

Bei Websites wird bei einer verschlüsselten Übertragung in der Adresszeile des Browsers nicht mehr bloss HTTP angezeigt, sondern HTTPS, ergänzt um ein grünes Schloss-Symbol. Damit ist die Übertragung der Original 1'000-er Note sichergestellt – **inklusive automatischer Rückmeldung der Seriennummer**.

Ohne Zertifikat	
Mit Zertifikat 1-4	
Mit Zertifikat 5	

Je nach Zertifikat wird die verschlüsselte Übertragung mit unterschiedlichen Symbolen in der Adresszeile des Browsers dargestellt.
Zertifikate: 1-4: Let's Encrypt oder DV oder Wildcard oder OV – Zertifikat 5: EV

Wer profitiert von der TLS-Verschlüsselung?
Nebst der erwähnten technischen Sicherheit ist das Symbol in der Adresszeile des Browsers auch ein vertrauensbildendes Zeichen an die Sitebesucher. Insbesondere bei Online-Shops und dort, wo Passworte eingegeben oder Formulare ausgefüllt werden müssen, können Sitebesucher kontrollieren, ob der Betreiber einer Website tatsächlich derjenige ist, für den er sich ausgibt.

Wie wird ein TLS-Protokoll eingerichtet?
Das Einrichten eines TLS-Protokolls geschieht über den Web-Hoster und ist ein rein technisch-administrativer Vorgang. Danach folgt jedoch noch Arbeit für den Webmaster. Er muss zum Beispiel die ausgehenden Links prüfen und allenfalls auf HTTPS umstellen, er muss in der Google Search Console die URL von HTTP auf HTTPS anpassen und allenfalls Google-Fonts und Google-Maps neu verlinken.

Werden diese Anpassungen nicht vorgenommen, wird das grüne Schloss in der Adresszeile des Browsers durch ein gelbes Schloss ersetzt. Das bedeutet, dass nicht alle Inhalte der jeweiligen HTML-Datei durchgängig mit HTTPS-Verknüpfungen versehen sind.

Was kostet das?
Die Zertifikate selber kosten zwischen einer kleinen Einrichtpauschale bis zu mehreren Hundert Franken pro Jahr. Die Kosten sind abhängig von der Validierung des Sitebetreibers. Diese kann einfacher Natur sein (Let's encrypt Zertifikat) oder sehr aufwändig ausfallen (EV-Zertifikat). Je aufwändiger übrigens, umso sicherer für den Sitebesucher.

Was meint Google dazu?
Google hat in einem Firmenblog mitgeteilt, dass der Browser «Chrome» (Marktanteil Schweiz über 36%) mit Release 68, also ab Sommer 2018, mit einem deutlichen Warnhinweis

«Die Verbindung zu dieser Website ist nicht sicher»

auf eine fehlende TLS-Verschlüsselung hinweisen wird. Andere Browser werden wahrscheinlich innert ein paar Wochen nachziehen.

Fazit
Wer für seine Website noch kein TLS-Zertifikat einsetzt oder zum Beispiel nur den Shop-Teil damit absichert, sollte nicht mehr zuwarten. Die drohenden Vertrauensverluste sowie abschreckende Warnhinweise wiegen bestimmt schwerer als eine relativ preiswerte Absicherung mittels eines TLS-Zertifikats.

---

webstyle

Weitere Informationen
tls.webstyle.ch

Kontakt
Webstyle GmbH, 3400 Burgdorf
Alain Martinet, Leiter Kundendienst
Telefon +41 34 423 00 00
www.webstyle.ch
