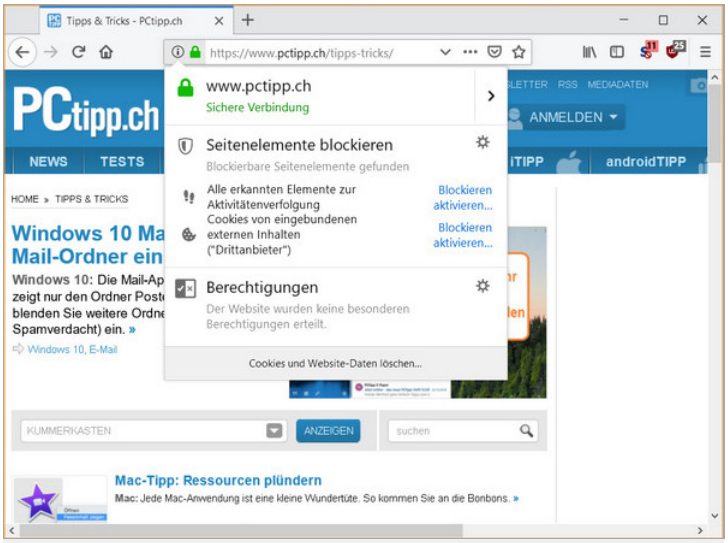
Sicherheit beim Surfen: Das Wichtigste rund ums Schloss-Symbol

Was genau bedeutet das Schloss-Symbol im Browser? Was ist der Unterschied zwischen http und https? Und wie prüfen Sie die angezeigten Zertifikate? Alle diese Fragen drehen sich um die Sicherheit beim Surfen. Wir geben Ihnen die Antworten.

von Gaby Salvisberg 19.06.2019

Elektronische Sicherheitszertifikate kommen an vielen Orten zum Einsatz. Ganz generell dienen sie dazu, die Echtheit einer Webseite oder auch einer Person festzustellen. Der mit dem Zertifikat verknüpfte öffentliche Schlüssel dient bei Webseiten zudem der verschlüsselten Datenübertragung. Seit Anfang November ist auch die PCtipp-Webseite (**pctipp.ch** (https://www.pctipp.ch/)) mit einer Verschlüsselung ausgestattet.



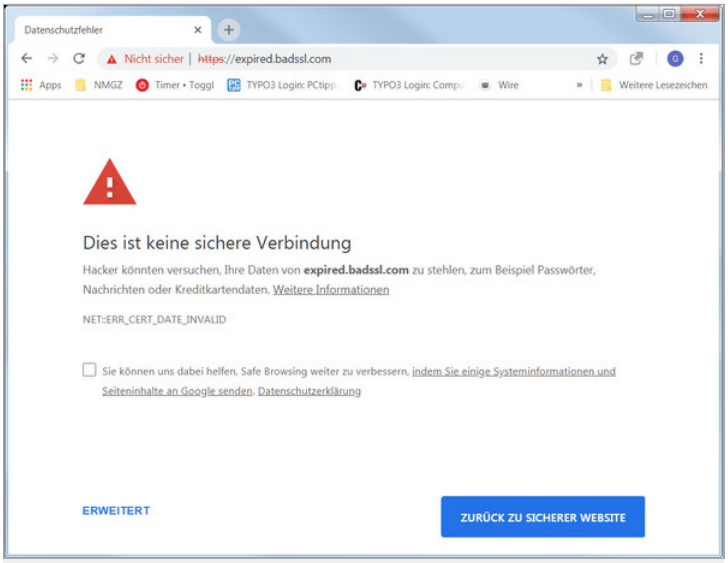
Auch die PCtipp-Website hat das grüne Schloss-Icon in der Adresszeile; es weist auf eine verschlüsselte Verbindung hin
© PCtipp

Wenn Sie früher per Webbrowser mit einer Webseite kommunizierten, kam üblicherweise das HyperText Transfer Protocol zum Einsatz, kurz http. Dieses hat jedoch einen gewichtigen Nachteil: Jeder, der sich im gleichen Netzwerk wie Sie bewegt, kann mit simplen Gratisprogrammen alle Daten mitschneiden, die Sie mit einer Webseite via http austauschen. Bei profanen Dingen wie Fahrplanabfragen, dem Lesen von News oder beim Nachschlagen in einem Onlinelexikon mag das nicht so schlimm sein. Sehr viele Daten, die Sie mit Webseiten austauschen, sind jedoch privater Natur. Da wären zum Beispiel Passwörter, die Sie zum Einloggen auf Webseiten benutzen. Die dürfen keinesfalls in fremde Hände gelangen. Noch heikler wird es beim Internetbanking, beim Besuch Ihres Krankenkassen-Accounts, bei Einkäufen oder bei Benutzung von Webmail für die private Korrespondenz. Würde dies bloss via http abgewickelt, könnten Mitlauscher Ihre Finanz- und Krankheitsdaten abgreifen und Ihre E-Mails lesen.

Darum wurde das Protokoll um eine Sicherheitsschicht erweitert. Geboren war das HyperText Transfer Protocol Secure, kurz https. Hierbei handelt es sich um eine sogenannte Transportverschlüsselung, in der Fachsprache Transport Layer Security (TLS) genannt. Anders als etwa in der E-Mail-Verschlüsselung (Pretty Good Privacy, PGP) brauchen sich die Benutzer bei https nicht selbst um irgendwelche Schlüssel zu kümmern. Ihr Webbrowser und der Webserver, den Sie damit besuchen, handeln die Sache mit den Schlüsseln in Sekundenbruchteilen selbst aus.

Wie funktioniert das?

Angenommen, Sie besuchen eine Webseite, zum Beispiel **pctipp.ch** (https://www.pctipp.ch/) . Wie jede Webseite liegt auch diese auf einem Webserver. Ihr Browser meldet sich beim Webserver, mit dem Wunsch, pctipp.ch via https abzurufen. Der Webserver übermittelt an Ihren Browser das zu pctipp.ch gehörende Zertifikat. Darin enthalten ist der öffentliche Schlüssel des Webauftritts. Ihr Webbrowser überprüft das Zertifikat, um herauszufinden, ob es sich wirklich um pctipp.ch handelt. Wenn diese Prüfung erfolgreich verläuft, erstellt der Browser einen Sitzungsschlüssel. Den verschlüsselt er mit dem öffentlichen Schlüssel des Webservers und stellt ihm diesen zu. Damit haben sich Webbrowser und Server auf einen symmetrischen Sitzungsschlüssel geeinigt, mit dem der Webseitenbesuch beiderseits verschlüsselt wird. Allfällige Mitlauscher bekommen nur Zahlen- und Buchstabensalat zu sehen.
Wichtig: Bloss weil eine Webseite ein gültiges Zertifikat hat, muss das noch nicht bedeuten, dass der Anbieter seriös ist. Es heisst nur, dass für die angegebene Domain ein gültiges Zertifikat implementiert wurde. Er kann Sie also dennoch mit gefälschten Angeboten oder anderen Tricks über den Tisch ziehen.



Es müssen nicht gleich Hacker am Werk sein, wenn das Zertifikat einer Website nicht gültig ist
© PCtipp

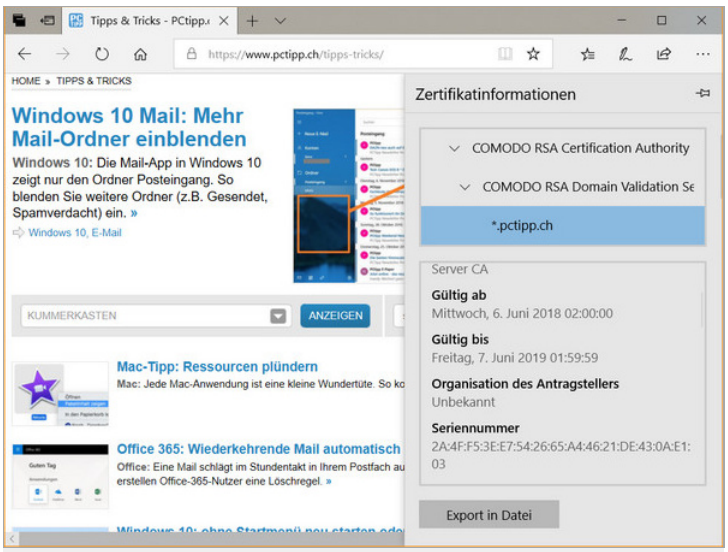
Wenn die Zertifikatsprüfung im Webbrowser hingegen scheitert, erscheint im Browser eine Fehlermeldung, die oftmals ziemlich furchteinflössend klingt. Meistens ist ein Besuch der Seite aber mit den richtigen Klicks trotzdem möglich. Ratsam ist der Besuch aber nicht, falls Sie vorhaben, mit der Webseite private Daten auszutauschen oder falls es sich um einen Shop handelt. Die Gründe für ein Scheitern der verschlüsselten Verbindung sind aber manchmal relativ harmlos. Unten zwei häufig angetroffene Beispiele.

- **Falsche Domain:** Vielleicht wurde ein Zertifikat bloss auf «www.example.com» ausgestellt, nicht aber auf «webmail.example.com», das aber offensichtlich auch Teil der Domain «example.com» ist. In so einem Fall hat es die Firma «example.com» schlicht verpasst, das Zertifikat für ihre gesamte Domain (*.example.com) ausstellen zu lassen (siehe Stichwort «wrong.host» am Ende des letzten Absatzes in diesem Artikel).
- **Gerade abgelaufen:** Elektronische Zertifikate haben immer ein Ablaufdatum. Jemand, der beim Webseitenbetreiber diese Daten im Auge behalten sollte, hat das Erneuern verschlafen. Sobald das Zertifikat abgelaufen («expired») ist, sehen die Nutzer ebenfalls die Meldung, das Zertifikat sei ungültig. Prüfen Sie es nach: Wenn es eben erst (also gerade in den letzten ein, zwei Tagen) abgelaufen ist, informieren Sie die Firma unbedingt darüber. Wenn es die richtige Domain der Firma ist, dann dürfte ein Fortsetzen des Webseitenbesuchs weiterhin harmlos sein. Ausser, es sei eine Bank oder Versicherung. Einem Geldinstitut darf das mit der verpassten Zertifikatserneuerung auf gar keinen Fall passieren.

Nächste Seite: Info anschauen und Weitere Tipps

Info anschauen

Wenn ein Zertifikat gültig ist, können Sie es sehr einfach prüfen. In den drei Webbrowsern Edge, Chrome und Firefox klicken Sie zunächst auf das *Vorhängeschloss*-Icon vor der Webadresse. Im Windows-10-Webbrowser Edge gehen Sie nun zu *Zertifikat anzeigen*. Sie finden darin das Unternehmen, welches das Zertifikat für die Webseite ausgestellt hat. Weiter ist dort auch das Ablaufdatum (*Gültig bis*) zu sehen. Darunter finden Sie nebst elektronischen Fingerabdrücken auch den öffentlichen Schlüssel, den wir unter «Wie funktioniert das?» erwähnt haben.



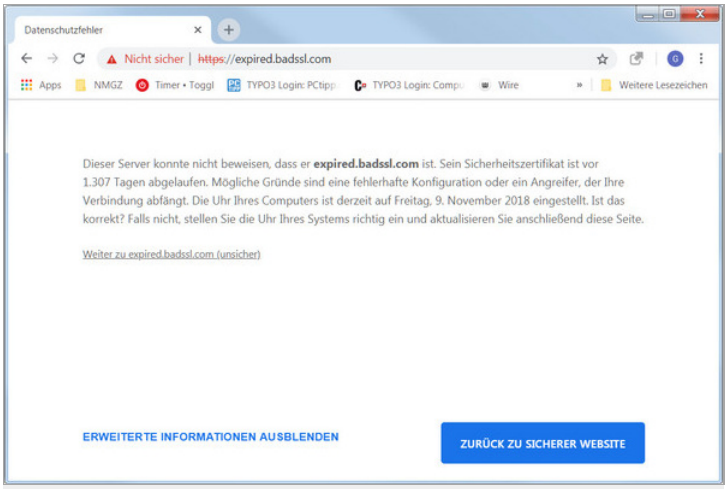
Beispiel Microsoft Edge – für die Domain pctipp.ch wurde das Zertifikat von Comodo ausgestellt. Es ist bis Juni 2019 gültig
© PCtipp

In Googles Chrome-Browser gehen Sie nach dem Klick auf das *Schloss*-Symbol zu *Zertifikat (gültig)*. Jetzt erscheint ein neues Fenster, das in Reitern wie *Details* und *Zertifizierungspfad* dieselben Informationen liefert.

In Mozilla Firefox steuern Sie nach dem Klick aufs *Schloss* zum nach rechts weisenden Winkel hinter *Sichere Verbindung*. Die Option *Weitere Informationen* öffnet ein neues Fenster. Die Schaltfläche *Zertifikat anzeigen* enthüllt wieder die bekannten Zertifikatsinformationen.

Falls der Browser hingegen bezüglich des Zertifikats meckert, müssen Sie sich das Zertifikat anschauen, um herauszufinden, was krumm ist. Vielleicht wird dadurch klar, dass es ein plausibler, aber harmloser Grund ist, der den Browser zum Meckern bringt. Das geht in den Webbrowsern Chrome, Edge und Firefox wie folgt:

- **Google Chrome:** Google Chrome titelt die Meldung mit *Dies ist keine sichere Verbindung*. Klicken Sie unten aufs unscheinbare Wort *Erweitert*. Chrome zeigt an, warum er das Zertifikat fürungültig hält. Falls Sie mit der Webseite keine wichtigen Daten austauschen und darauf auch keine Einkäufe tätigen wollen, können Sie unten auf den Link namens *Weiter zu example.com (unsicher)* klicken.



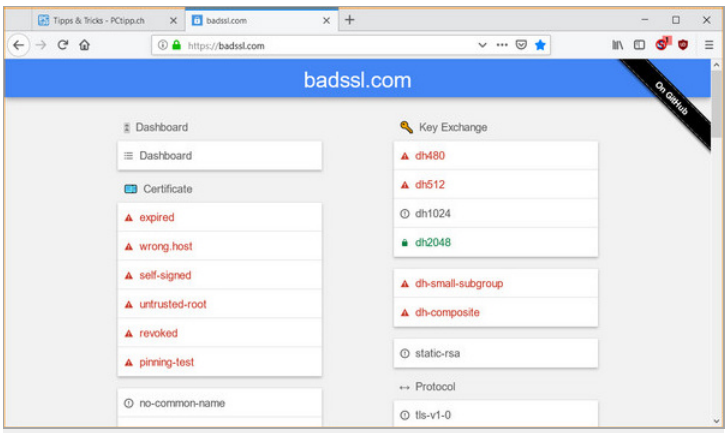
Googles Chrome-Webbrowser – mit der Option Weiter zu … gelangen Sie dennoch auf die Webseite
© PCtipp

- **Microsoft Edge:** Dieser Browser meldet *Diese Website ist nicht sicher*. Klicken Sie aufs *Warndreieck* vor der Adresse und gehen Sie zu *Zertifikat anzeigen*. Alternativ können Sie auf *Details* klicken, dann schreibt Edge zum Beispiel hin: *Das Sicherheitszertifikat der Webseite ist abgelaufen oder noch nicht gültig.* Darunter gibt es – falls Sie der Seite trauen – den Link *Webseite trotzdem laden*.
- **Mozilla Firefox:** Er setzt die Hürden bei Zertifikatsproblemen etwas höher. Zunächst meldet er *Diese Verbindung ist nicht sicher*. Klicken Sie auf *Erweitert*, erfahren Sie oft schon den Grund. Wollen Sie die Seite dennoch besuchen, müssen Sie unten eine Ausnahme hinzufügen.

Weitere Tipps

Falls Sie für einen Webauftritt zuständig sind, dürfte es Ihnen obliegen, sich um das Problem zu kümmern. Sprechen Sie mit Ihrem Web- oder Mailhoster. Er kann Ihnen beim Erstellen und Einbinden eines Zertifikats bestimmt helfen. Falls Sie Subdomains (*shop.example.com, mail.example.com* etc.) verwenden, achten Sie beim Ausstellen des Zertifikats darauf, dass es für Ihre ganze Domain (**.example.com*) gilt und nicht nur für eine Subdomain bzw. einen einzelnen Hostnamen. Tragen Sie in Ihren Kalender eine Erinnerung ein, die Sie ein bis zwei Wochen vor Ablauf des Zertifikats ermahnt, die Erneuerung durchzuführen.

Wollen Sie einmal testen, wie Ihr Webbrowser reagiert, wenn er auf dieses oder jenes Zertifikatsproblem trifft? Auf der Site **https://badssl.com** (https://badssl.com/) finden Sie im Bereich *Certificate* ein paar Links, welche die erwähnten Zertifikatsfehler nachstellen. Klicken Sie zum Beispiel auf *expired*, landen Sie auf einer Testseite mit absichtlich abgelaufenem Zertifikat. Der Link *wrong.host* führt zu einer Subdomain, die im ansonsten gültigen Zertifikat der Domain nicht enthalten ist.



Badssl.com ist eine Webseite mit absichtlich falschen Zertifikaten. Damit können Sie das Verhalten Ihres Browsers testen
© PCtipp