SSL Sicherheit

Hinweise zur Sicherheit der SSL-verschlüsselten Datenübermittlung

Meier Informatik
Rainer Meier
Mühlistr. 4
6288 Schongau
skybeam@skybeam.ch

2014-04-04

1. Inhaltsverzeichnis

2. Einleitung

Beim Abruf von Daten aus dem Internet kann zwischen unverschlüsselter und verschlüsselter Übertragung unterschieden werden. Für die Verschlüsselung wird allgemein meist SSL (Secure Socket Layer) verwendet. Manchmal wird auch der Begriff TLS (Transport Layer Security) verwendet. Für dieses Dokument ist es aber synonym zu verwenden. SSL/TLS stellt eine abhörsichere Ende-zu-Ende Verschlüsselung zwischen zwei Kommunikationspartner sicher.

Bei SSL-verschlüsselten Verbindungen (HTTPS) wird eine direkte Verbindung zwischen zwei Kommunikationspartnern erstellt. Die verschlüsselte Verbindung wird aufgebaut noch bevor Daten wie Passwörter zwischen den Kommunikationspartnern ausgetauscht werden. So wird sichergestellt, dass alle ausgetauschten Daten nur dem jeweiligen Kommunikationspartner eingesehen werden können.

Um das Prinzip zu veranschaulichen verwenden wir hier ein Beispiel der verschlüsselten SSL-Verbindung mit Google.

Abbildung 1 SSL/HTTPS Verbindung

Die Verbindungsdaten werden im Netzwerk komplett verschlüsselt übertragen. Die Daten können zwar abgehört aber von niemandem entschlüsselt oder gar verändert werden. Der Benutzer ist sicher, dass alle zu Google gesendeten Daten nur von Google gelesen werden können (z.B. Passwörter und persönliche Daten wie Sucheingaben oder Mails) und die Antworten von Google ebenfalls weder abgehört noch verändert werden können.

Um die Daten dennoch abhören und verändern zu können wird nun ein sogenannter Man-In-The-Middle (MITM) Angriff durchgeführt. Solche Angriffe werden üblicherweise von dritten vorgenommen um an die übermittelten Daten zu gelangen und sind illegal. Aber auch Firmen setzen solche Systeme ein um die verschlüsselten Daten von- und zum Internet analysieren zu können. Die betroffenen müssen hier aber informiert werden und üblicherweise dem Einsatz solcher Systeme zustimmen (meistens über Mitarbeiter-Vereinbarungen geregelt). Da ein solches System die Privatsphäre sowie Sicherheit der übertragenen Daten gefährdet sollten sich die Mitarbeiter bewusst sein, dass ihre Daten dadurch von dritten gelesen werden können. Dies schliesst alle übertragenen Daten wie Formulareingaben, Suchanfragen, e-Mails, Online-Kommunikation, Passwörter usw. ein.

3. Man-In-The-Middle (MITM) Angriff

Anstatt die Daten an Google zu übermitteln werden die Verbindungen über ein System eines Angreifers umgeleitet und werden dann nicht mehr direkt zu Google übertragen:

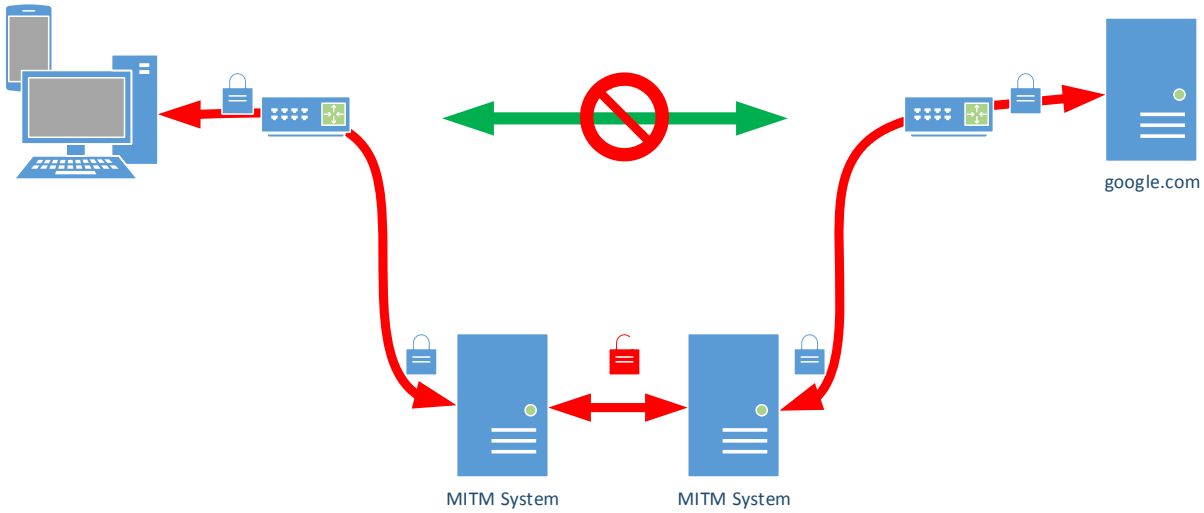


Abbildung 2 Man-In-The-Middle (MITM) Angriff auf verschlüsselte Verbindungen

Wie hier zu sehen ist findet die Verbindung nun nicht mehr zwischen dem Benutzer und Google statt sondern wird an das MITM-System umgeleitet. Dier Verbindung vom Benutzer zum MITM System findet zwar verschlüsselt statt aber nur bis zu diesem System. Das MITM-System kann jetzt die Daten vom Benutzer entschlüsseln, mitschneiden/protokollieren oder gar verändern. Dann leitet das System die empfangenen Daten stellvertretend zu Google weiter. Google kann aber nicht feststellen ob die Anfrage vom Benutzer oder von dem MITM-System stammt und beantwortet die Anfrage. Die Kommunikation zwischen dem MITM-System und Google findet wiederum verschlüsselt statt. Die Antwort von Google wird dann wieder entschlüsselt, protokolliert, ggf. verändert und an den Benutzer zurückgeliefert.

Als Folge davon findet nie eine sichere Verbindung zwischen dem Benutzer und Google statt. Alle Daten sind auf dem MITM-System unverschlüsselt protokollierbar, einsehbar und auch veränderbar. Der Benutzer ist zu keinem Zeitpunkt auf einem sicheren Kanal mit Google verbunden.

Der Benutzer kann diesen Eingriff allerdings erkennen. Das von Google an den Benutzer gelieferte Sicherheitszertifikat wird durch das MITM-System ersetzt und ist nicht als vertrauenswürdig für die aufgerufene Seite eingestuft. Der Benutzer wird dann in der Regel auf ein ungültiges Zertifikat hingewiesen und kann entscheiden ob die Verbindung abgebrochen werden soll oder ob trotzdem fortgesetzt werden soll. In Firmen bei denen MITM eingesetzt wird sind die Arbeitsplätze häufig schon so modifiziert, dass die entsprechende Sicherheitswarnung unterdrückt wird oder das gefälschte Sicherheitszertifikat als echt akzeptiert wird. Der Benutzer kann also nur durch manuelle Überprüfung feststellen, ob das Sicherheitszertifikat gefälscht ist oder wirklich von der aufgerufenen Seite stammt. Diese Überprüfung

Wie erwähnt betreiben auch einige Firmen MITM Systeme. Meistens wird als Grund die Sicherheit genannt damit alle übertragenen Daten überprüft werden können. Den Firmen geht es dabei weniger um die Sicherheit der Mitarbeiter bzw. deren IT-Ausstattung sondern um die übertragenen Firmendaten. Dem Mitarbeiter sollte bewusst sein, dass die Firma dann auch Einblick in alle übertragenen Daten erhält und auch sehen kann welche Daten mit einem Facebook-Chatpartner oder auf dem privaten E-Mail ausgetauscht werden.

Wer seiner Firma hier voll vertraut sollte trotzdem skeptisch sein denn durch die aufgebrochenen Verschlüsselung ist es für den Benutzer auch unmöglich weitere Manipulationen zu erkennen. Beispielsweise wenn die Firmen-Systeme ebenfalls von dritten manipuliert wurden oder die Firma selbst Opfer seines solchen MITM-Angriffs wurde:

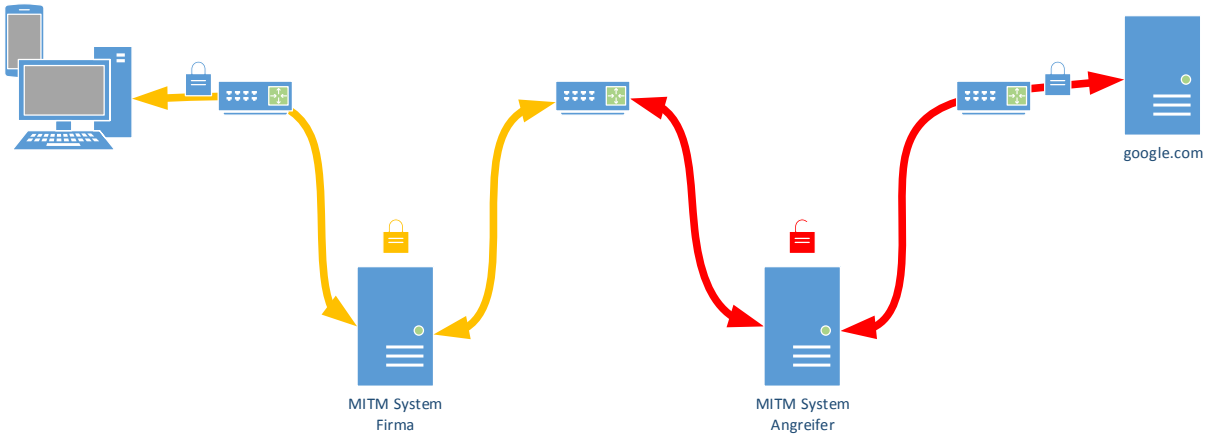


Abbildung 3 Angriff eines unsicheren Systemes

In einem solchen Fall kann der Benutzer den Angriff nicht erkennen weil seine Verbindung vermeintlich sicher mit dem Zertifikat vom MITM System der Firma stattfindet.

Einzig das MITM-System der Firma könnte in so einem Fall die Manipulation durch den Angreifer feststellen und die Verbindung abbrechen. Da dies aber weitere Seiteneffekte mit Seiten ohne gültiges Zertifikat hätte wird dies kaum gemacht. Daher ist es dem Benutzer nicht möglich festzustellen ob nur die Firma oder noch weitere Dritte Zugriff auf die Daten erlangen.

Weitere Probleme ergeben sich mit Diensten welche eine sichere Kommunikation erzwingen. Beispielsweise kennt der Google Browser Chrome das offizielle Zertifikat von Google und lehnt in jedem Fall eine Verbindung über ein gefälschtes Zertifikat ab. Ebenso kann es passieren, dass Mobiltelefone (z.B. Android) ihre Daten nicht synchronisieren können weil die Verbindung vom Gerät abgebrochen wird. Beispielsweise werden dann Kontakte und Kalender-Einträge nicht automatisch zwischen Mobiltelefon und Tablet synchronisier.

4. Technische Umsetzung

Damit das funktioniert muss sich das MITM-System gegenüber dem Benutzer natürlich als Google-System zu erkennen geben (Identitätsfälschung). Diese Fälschung wird von aktuellen Webbrowsern erkannt und eine entsprechende Warnung ausgegeben. Hier exemplarisch die Warnung von Firefox:

Abbildung 4 Zertifikatswarnung von Google

Im Abschnitt Technische Details steht auch der Grund für die Warnung: www.google.ch verwendet ein ungültiges Sicherheitszertifikat. Dem Zertifikat wird nicht vertraut, weil das Aussteller-Zertifikat unbekannt ist.

Aber was heisst das jetzt:

Zertifikate werden von vertrauenswürdigen Stellen ausgegeben. Firefox kennt die Zertifikatsaussteller (Certificate Authority, CA) welche das Zertifikat für google.ch ausgestellt haben. Diese vertrauenswürdigen CAs würden niemals ein Zertifikat für die Seite google.ch an jemand anderen als an Google geben. In dem Fall betreibt aber eine Drittperson das MITM-System und benötigt ein Zertifikat für google.ch. Nun wird dies schlicht gefälscht und von einer eigenen (für Firefox nicht vertrauenswürdigen) Zertifizierungsstelle unterschrieben. Firefox stellt nun also fest, dass die angebliche Verbindung mit google.ch eben nicht mit Google verbindet sondern mit einem unbekannten System.

Ein Klick auf „Ausnahmen hinzufügen…“ erlaubt uns entweder das falsche Zertifikat zu akzeptieren oder auch genauer zu analysieren. Ein Klick auf „Ansehen“ im erscheinenden Dialog zeigt dann die Zertifikats-Details:

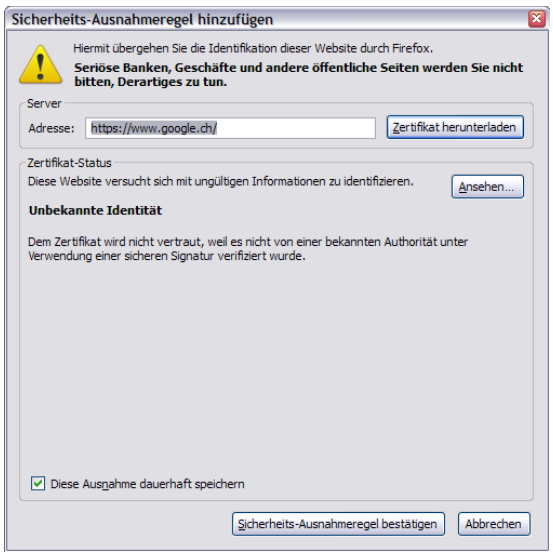


Abbildung 5 Ausnahme hinzufügen

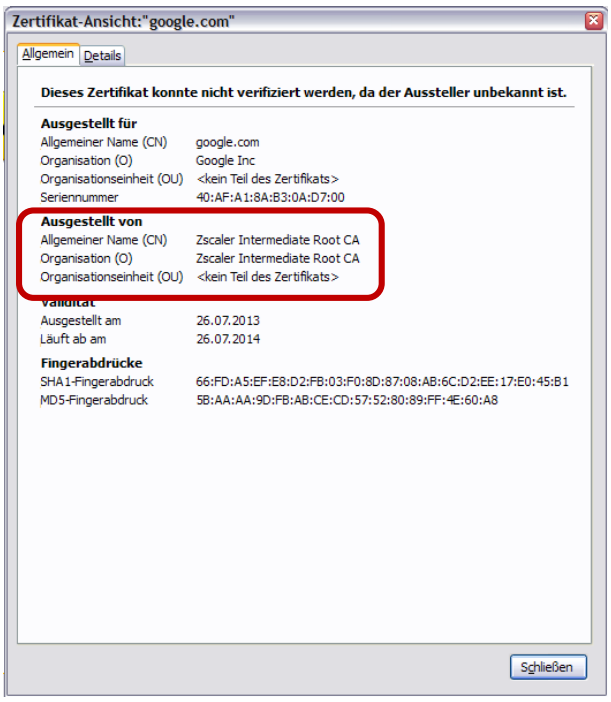


Abbildung 6 Gefälschtes Zertifkat

Wie auf dem Bild zu sehen ist wurde das gefälschte Zertifikat von „Zscaler Intermediate Root CA“ ausgestellt. Hier zum Vergleich das vertrauenswürdige Zertifikat von Google selbst:

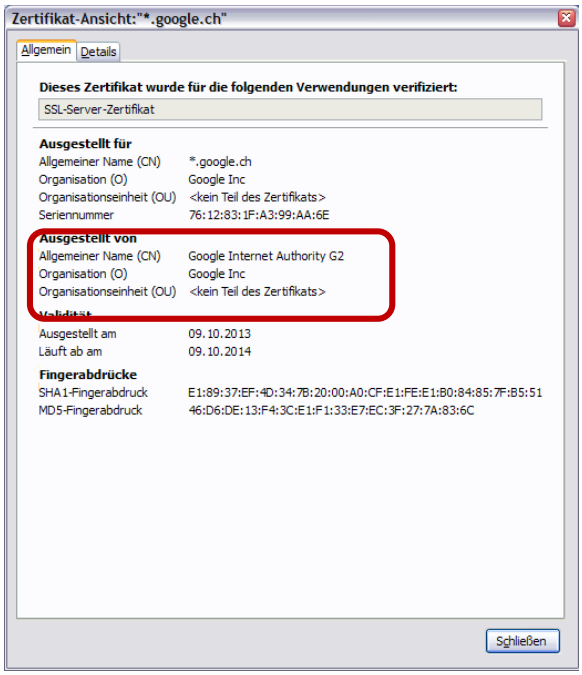


Abbildung 7 Echtes Google Zertifikat

Wie zu sehen ist wird das echte Google-Zertifikat von Google ausgestellt.

Klickt man im obigen Ausnahme-Dialog auf „Sicherheits-Ausnahmeregel bestätigen“ wird Firefox dieses gefälschte Zertifikat akzeptieren und in Zukunft nicht mehr warnen. Dies kann auch temporär geschehen indem man die Auswahl vor „Diese Ausnahme dauerhaft speichern“ entfernt.

Wer eine Ausnahmeregelung hinzufügt und das gefälschte Zertifikat akzeptiert muss sich bewusst sein, dass die Daten nicht auf einem sicheren Kommunikationskanal zur aufgerufenen Seite gelangen sondern möglicherweise von dritten gelesen, gespeichert oder manipuliert werden können.

5. Massnahmen

Wenn keine Sichere Verbindung zum gewünschten System stattfinden kann, dann hat man als Benutzer nur zwei Möglichkeiten. Entweder die unsichere Verbindung zu akzeptieren oder den Dienst nicht zu nutzen. In der Regel sollte man sich dann entscheiden die Verbindung abzubrechen:

Abbildung 8 Unsichere Verbindung abbrechen

Dadurch kann man zwar den Dienst nicht nutzen aber man verhindert wenigstens, dass Passwörter und Daten in Hände dritter gelangen. Insbesondere bei sensiblen Seiten wie e-Banking und anderen sensiblen Seiten sollte man niemals eine Ausnahme hinzufügen und die Verbindung immer beenden.

Aber auch bei vermeintlich unkritische Seiten wie Google, Facebook, Twitter, Webmail usw. sollte man sich bewusst sein, dass die Daten in falsche Hände gelangen können und damit Schaden angerichtet werden kann. Von harmlosen Einträgen über ein gekapertes Twitter Konto bis zum vollständigen Identitätsdiebstahl mit Übernahme von E-Mail, Facebook-Konto oder auch Fremdbestellungen auf Seiten wie Amazon oder anderen Online-Shops auf Ihren Namen.

Ein möglicher Ausweg ist es ein anderes Netzwerk zu verwenden welches keine solchen Systeme einsetzt. Beispielsweise kann man (sofern verfügbar) mit einem anderen WLAN-Netzwerk verbinden oder auf Mobiltelefonen ganz auf WLAN verzichten und die Daten über Das Mobilfunknetz übertragen. Dies kann dann aber je nach gewähltem Mobilfunkvertrag weitere Kosten verursachen.

6. Zertifikat entfernen

Wenn das Zertifikat durch den Benutzer permanente Ausnahme aufgenommen wurde akzeptiert Firefox das gefälschte Zertifikat von nun an ohne nachzufragen. Firefox blendet dann aber oben links neben der Adresszeile ein graues Schloss ein (bei gültigen Zertifikaten ist dies blau oder bei manchen e-Banking Seiten sogar grün wenn deine tiefere Zertifizierung der Seite stattgefunden hat).

Ein Klick auf das Schloss zeigt dann die Details an:

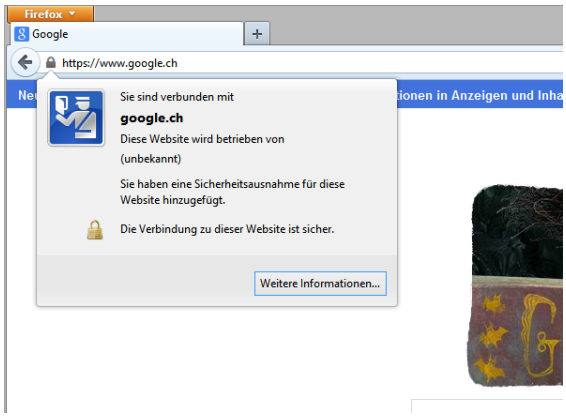
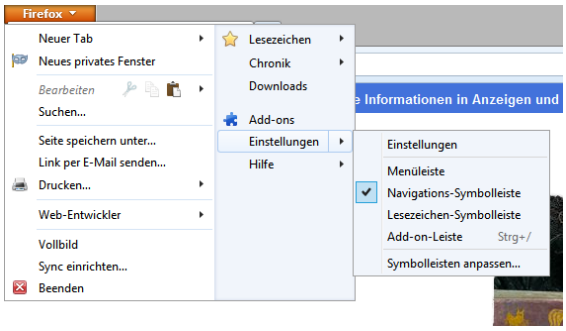


Abbildung 9 Manuelle Ausnahme bestätigt

Wie zu sehen ist wird das Zertifikat zwar akzeptiert aber der Betreiber der Seite wird als unbekannt ausgewiesen und ein Hinweis eingeblendet, dass eine Sicherheitsausnahme hinzugefügt wurde.

Die Sicherheitsausnahme kann wie folgt wieder entfernt werden:



Aufruf der Firefox-Einstellungen über das Firefox Menü. Menüeintrag „Einstellungen“ anklicken.

Abbildung 10 Firefox Einstellungen aufrufen

Dann über den Einstellungs-Dialog die gespeicherte Zertifikats-Ausnahme löschen:

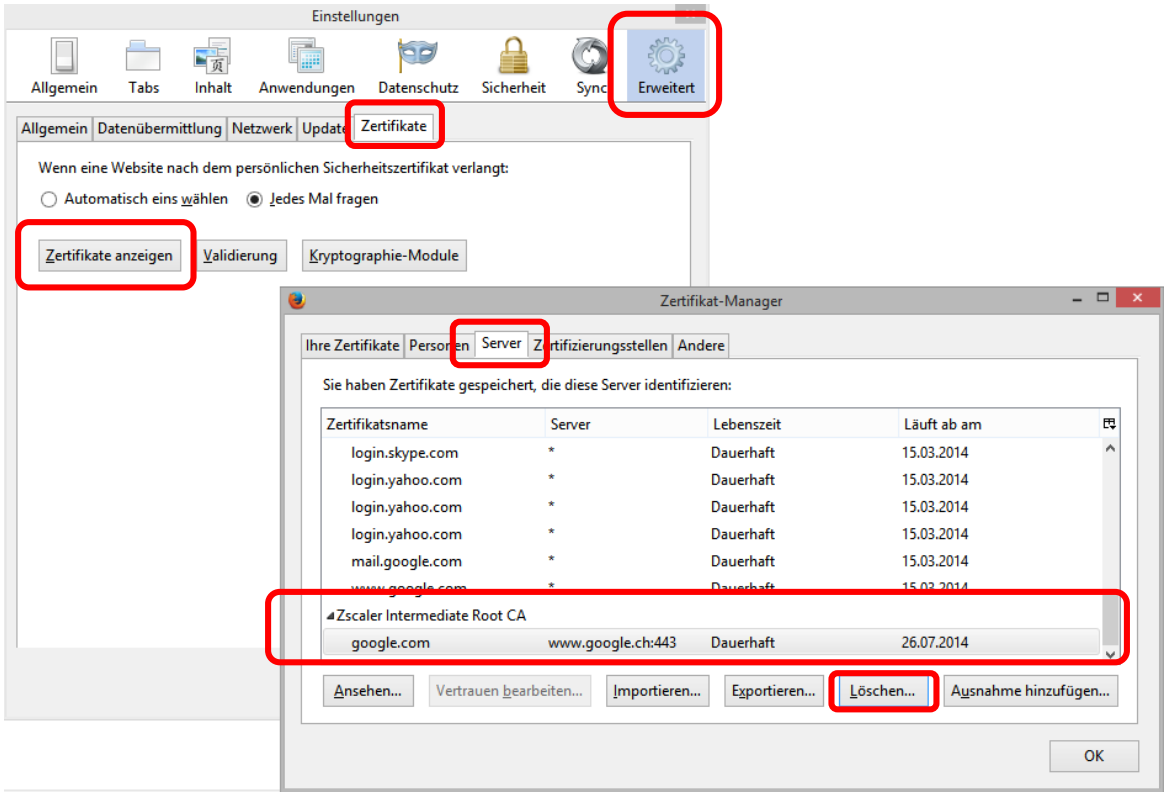


Abbildung 11 Zertifikats-Ausnahme löschen

Um das Zertifikat wieder zu löschen muss im Einstellungsmenü unter „Erweitert“ im Register „Zertifikate“ auf „Zertifkate anzeigen“ geklickt werden. Hier dann im Register für die Server-Zertifikate das entsprechende Zertifikat in der von Zscaler für google.com markieren und löschen.

Natürlich wird dadurch auch keine sichere Verbindung mit Google möglich aber der Browser warnt wieder vor dem gefälschten Zertifikate beim Zugriff auf die Google-Suche.

7. Anhang

7.1. Abbildungsverzeichnis