Die Sache mit den Zertifikaten

Wir bieten die meisten Dienste nur über verschlüsselte Verbindungen an. Und das ist auch gut so. Das Problem dabei ist: Dein Browser kann zwar eine verschlüsselte Verbindung aufbauen. So richtig sicher ist das aber nur, wenn er (bzw. du) auch wissen, dass am anderen Ende wirklich der Server ist, den Du dort erwartest.

Sonst könnte sich nämlich jemand dazwischen hängen. Die Verbindung wäre dann zwar verschlüsselt - aber nur von Dir bis zu der Frau oder dem Mann in der Mitte. Webadressen (urls) sind manipulierbar und reichen nicht aus, um sicher zu gehen dass du du auch wirklich mit dem Server verbunden bist mit dem du glaubst auf direktem Wege verbunden zu sein.

Dafür gibt es Zertifikate. Meistens funktioniert das so, dass irgend eine Firma, ein sog. Trustcenter (z.B. die Telekom) einem Webseitenbetreiber ein sogenanntes Zertifikat unterschreibt. Dieses Zertifikat präsentiert der Websever dem Browser, der die Unterschrift überprüft. Damit das funktioniert, muss dein Computer bzw. dein Browser (z.B. Firefox, Safari oder Internet Explorer) die digitale Unterschrift z.B. der Telekom bereits kennen. Bei vielen Verbindungen funktioniert das ohne weiteres: dann erscheint ein grünes oder blaues Feld in der Adressleiste und / oder ein Schloss. Dass das so ist liegt daran, dass die Browser-Hersteller bestimmte Wurzelzertifikate von sogenannten „vertrauensvollen“ Zertifikatsinstanzen schon in die Browser integriert haben. Eigentlich eine gute Sache. Aber sie hat einen Haken. Oder mehrere:

- Die Trustcenter machen das nicht umsonst. Zertifikate kosten z.T. aberwitzig viel Geld
- Wer kontrolliert die Trustcenter?
- Warum sollte mensch Zertifizierungsstellen trauen, die mensch nicht einmal dem Namen nach kennt?

In der Tat gibt es mittlerweile einige Trustcenter, die als „kompromittiert“ gelten[1)]. Das heißt, deren Stammzertifikate sind mal in die falschen Hände gekommen und sind daher nicht mehr sicher. Und damit auch all die von diesen Stellen signierten Zertifikate. Trotzdem geht das Geschäft oft weiter - die Trustcenter sind schlicht und einfach „too big to fail“ (das kennen wir auch von Banken 😉). Wenn die Browser-Hersteller diese Zertifikate aus den Browsern entfernen würden, würde schlicht und einfach eine Menge im Internet (Internetbanking, Onlineshops, etc.) nicht mehr funktionieren. Daher bleiben sie drinnen.

Wir haben lange überlegt, wie wir das Problem mit den Zertifikaten lösen sollen. Schließlich haben wir uns dafür entschieden, unser eigenes Trustcenter aufzubauen. Das hat aber auch einen Haken: Dein Browser oder dein E-Mail-Programm kennt unser „Trustcenter“ (noch) nicht.

Das kannst Du aber ändern, indem du unser „Wurzelzertifikat“ in Deinem Browser installierst.

https://datenkollektiv.net/zertifikate/

Woher weißt du, dass dir in diesem Moment nicht ein falsches Zertifikat untergeschoben wird? Sicher kannst Du nur sein, wenn Du mit uns über einen zweiten Kanal (also z.B. auf Papier oder per Telefon oder persönlich) den sogenannten Fingerabdruck des Zertifikates abgleichst.

Und außerdem hast du den Fingerabdruck wahrscheinlich in einer Mail von uns bekommen.

Aber natürlich könnte auch diese Webseite und die E-Mail manipuliert oder gar nicht von uns sein. Da

beißt sich die Katze in den Schwanz. Du siehst: es ist nicht ganz einfach mit der Sicherheit. Was genau du jetzt tun sollst, können wir dir auch nicht sagen. Du könntest darauf vertrauen, dass es für einen Potentiellen Angreifer schon ganz schön schwer ist, mehrere Kanäle gleichzeitig zu manipulieren.

Wer ganz sicher gehen will, ruft uns an oder verabredet sich mit uns zum Kaffee! Ob wir dann wirklich wir sind?

1)

http://de.wikipedia.org/wiki/Man-in-the-Middle-Angriff
http://www.heise.de/security/meldung/DigiNotar-Hack-Kritische-Infrastruktur-war-unzureichend-geschuetzt-1337378.html