Die Sache mit den Zertifikaten

Hier steht ein bisschen was zur Theorie. Die Praxis findet sich unter Wurzelzertifikat installieren.

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. Deshalb haben wir früher unser eigenes „Trustcenter“ betrieben. Das hat aber nicht nur uns viel Arbeit gemacht - es war auch nicht besonders User*innen-freundlich. Das Thema Zertifikat war daher immer Support-Thema Nr. 1.

2016 haben dann unter Anderem die EFF und Mozilla das Projekt Let's Encrypt initiiert. Seit dem gibt es ein standartmäßig installiertes „Trustcenter“, welches massenhaft und kostenlos Zertifikate ausstellt und damit eine weitere Verbreitung von Verschlüsselung ermöglicht. Im Mai 2018 haben wir unsere Infrastruktur auf ein Let's Encrypt Zertifikat umgestellt, um den Aufwand der Installation und Authentifizierung unseres Wurzelzertifikats zu ersparen. Natürlich bleiben einige Probleme: auch dieses Trustcenter könnte kompromitiert sein, etc. Wir denken aber, dies ist aktuell ein vertretbarer Kompromiss zwischen Benutzer*innenfreundlichkeit und Sicherheit.

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
http://www.golem.de/1106/84369.html
http://www.golem.de/news/kaspersky-lab-wie-sich-geheimdienst-selbst-legitime-zertifikate-ausstellen-1308-101036.html