LU16b - HTTPS

Das **H**yper**T**ext **T**ransfer **P**rotocol **Secure** stellt eine vertrauliche Kommunikation zwischen Client und Server über SSL/TLS sicher. Dies wird unter anderem durch Verschlüsselung und Authentifizierung erreicht.

Zusätzliches Material

- Hypertext_Transfer_Protocol_Secure
- Video: SSL / TLS einfach erklärt

Authentifizierung

Für eine sichere Kommunikation muss zunächst sicher sein, dass der korrekte Webserver meine Anfragen erhält. Dazu muss sich der Server mit einem Zertifikat ausweisen, welches unter anderem den Domainnamen enthält. Nur wenn der Domainname im Zertifikat mit der aufgerufenen Domain übereinstimmt, wird eine sichere Kommunikation aufgebaut. Andernfalls zeigt mein Browser eine Warnung oder lehnt die Kommunikation komplett ab.

Das Ausstellen eines Zertifikats ist so einfach, dass jeder Serveradministrator beliebige Zertifikate erstellen kann. Sie könnten also einfach ein Zertifikat ausstellen, dass ihren privaten Server als den offiziellen Server der Eidgenossenschaft ausweist. Solche selbst ausgestellten Zertifikate werden natürlich von einem Webbrowser abgelehnt.

Zertifizierungsstelle

Damit ein Zertifikat akzeptiert ist, muss es von einer offiziellen Zertifizierungsstelle signiert werden. Diese Signatur bestätigt, dass die Zertifizierungsstelle das Zertifikat und die darin enthaltenen Angaben überprüft hat. Weil diese offiziellen Zertifikate teilweise recht teuer sind, hat sich HTTPS nur langsam verbreitet.

2015 ging die Zertifizierungsstelle Let’s_Encrypt online. Dieser gemeinnützige Dienst bietet kostenlose Zertifikate an. Ausserdem bietet Let's Encrypt für die meisten Betriebssysteme Skripts an, welche die Nutzung sehr einfach machen:

- Erstellen des Zertifikats
- Erneuerung des Zertifikats
- Konfiguration des Webservers

Verschlüsselung

Nachdem die Identität des Servers geprüft wurde, handeln Client und Server die Verschlüsselung aus. Dabei einigen sich Client und Server auf einen Verschlüsselungsalgorithmus und einen Schlüssel. Sämtliche Datenpakete werden anschliessend verschlüsselt übertragen.

---

m231-AnG