

Zertifizierungsstellen, Browser und das Geschäft mit SSL

Verschlüsselte Webseiten sind in der heutigen Zeit ein wichtiges Element um sensible Daten bei z.B. Bankgeschäften im Internet zu schützen. Leider kosten diese Zertifizierungen viel Geld obwohl die Aussage des Browsers: "Blabla.com verwendet ein ungültiges Sicherheitszertifikat" wenig bzw. nix über die tatsächliche Sicherheit der Verbindung aussagt. Oft sind Zertifikate die vom Browser als ungültig bezeichnet werden trotzdem sicherer als andere Zertifikate, die als gültig gekennzeichnet werden.

Mein Vorschlag wäre das Verfahren in zwei Teile zu gliedern. 1. Verschlüsselte Webseiten Jeder soll die Möglichkeit haben, seinen Besuchern eine sichere Verbindung zur Verfügung zu stellen, ohne das man dafür zahlen muss und der Browser das Zertifikat als invalid kennzeichnet. 2. Verschlüsselte und verifizierte Webseiten Es soll auch weiterhin die Möglichkeit geben Webseiten gegen Geld zu verifizieren. Somit kann sich der Besucher sicher sein, dass die Firma real existiert und es sich nichtum Betrüger handelt. Ausserdem könnte ich mir eine Art Ampelsystem vorstellen, das Aussagen über die Schlüsselstärke zur Verfügung stellt. Leider wird das in naher Zukunft kaum möglich sein, derzeit sind SSL Zertifikate ein gutes Geschäft, dafürspricht auch, dass die Browser den Zugang extrem erschwert haben. Früher war es möglich mit exakt einem Mausklick eine "nicht vertrauenswürdige Webseite" zu besuchen, heute ist es ein ewiges und nerviges rumgeklicke bis man irgendwann gnädigerweise doch auf die Webseite kommt. Bleibt zu hoffen, dass sich hier was ändern wird, da das jetzige Verfahren weder für den Endbenutzer noch für den Betreiber wirklich zielführend ist. Andreas <http://de.wikipedia.org/wiki/Zertifizierungsstelle> <http://www.openca.org>