Jimmy Schulz
Peter Simons

Handout zum Fachgespräch vertrauliche Kommunikation im Deutschen Bundestag am 03.09.2013

Session 3
Sichere Kommunikation per E-Mail

Die Sicherheit eines Kommunikationsmediums beurteilt man unter anderem danach, inwieweit die folgenden Eigenschaften gewährleistet sind:

1) Vertraulichkeit: Nachrichten sollen nur für den vorgesehenen Empfänger lesbar sein.

2) Authentizität: Der Empfänger muss die Identität des Absenders feststellen können.

3) Integrität: Nachrichten müssen den Empfänger unverfälscht erreichen.

Bei normaler E-Mail-Kommunikation ist *keine* dieser Eigenschaften gewährleistet: E-Mail bietet dem Nutzer dasselbe Sicherheitsniveau wie eine Postkarte.

Diese Situation lässt sich jedoch durch den bewussten Einsatz von Verschlüsselungssoftware deutlich verbessern. Das bekannteste Programm hierzu ist -- der GNU Privacy Guard (GPG) --, dieser ist unter <http://gnupg.org/> frei verfügbar.

Anleitung zur E-Mail Verschlüsselung anhand des Beispiels Thunderbird mit GnuPG und Enigmail:

Neben der hier besprochenen Variante gibt auch andere Methoden wie z. B. S/MIME. Wir wollen diese in eine der nachfolgenden Veranstaltungen im Laufe des Jahres vorstellen.

Benötigte Komponenten:

Thunderbird: http://www.mozilla.org/de/thunderbird/

GPG4WIN: http://www.gpg4win.de/

Enigmail: https://addons.mozilla.org/de/thunderbird/addon/enigmail/

Nach der Installation aller Komponenten ist lediglich Enigmail innerhalb Thunderbirds aufzurufen. Ab dann startet ein automatischer, Schritt-für-Schritt geleiteter Assistent, der einen Schlüsselpaar generiert. Insgesamt haben Sie am Ende drei „Schlüssel“:

1. Einen Öffentlichen, den Sie ihren Kommunikationspartnern geben können. Mit öffentlichen Schlüssel können Sie E-Mails verschlüsseln.

2. einen privaten Schlüssel: Dieser sollte sicher auf Ihrem Rechner, oder USB-Stick verwahrt werden. Dieser dient zum Entschlüsseln von E-Mails, die Sie empfangen.

3. Passwort: Dieses sichert den privaten Schlüssel zusätzlich ab. Also kann eine E-Mail nur entschlüsselt werden, wenn der private Schlüssel vorhanden ist und das Passwort eingegeben wurde.