E-Mail Verschlüsselung mit gpg/pgp und mit Zertifikaten

Es gibt grundsätzlich zwei Möglichkeiten, E-Mails Ende-zu-Ende zu verschlüsseln.

1. Mit gpg/pgp (vorwiegend im privaten Einsatz)
2. mit sog. X.509-Zertifikaten und Public-Key Infrastruktur (vorwiegend innerhalb von Organisationen)

Wir gehen auf beides ein und erklären hier, wie du dein E-Mail-Programm einrichten musst um verschlüsselte E-Mails zu verschicken.

Verschlüsseln mit pgp/gpg

Vorteile:

Nachteile:

- Das gundlegende Problem ist nur schwer lösbar: Wie kommt der öffentlich Schlüssel sicher zum Empfänger
- Öffentliche Schlüsselserver erleichtern zwar den Schlüsselaustausch - haben aber ein anderes Problem: Die Daten aus den Schlüsseln (also auch die E-Mail-Adressen) sind öffentlich. Sie werden zwar von Suchmaschinen in der Regel nicht gefunden. Aber nach dem ursprünglichen Konzept des Web of Trust funktioniert das ganze auch nur, wenn die Schlüssel wiederum von anderen signiert sind. Anhand der Signaturen können wiederum soziale Netzwerke rekonstruiert werden, was nicht immer gewünscht ist.

Verschlüsseln mit X.509-Zertifikaten

Der wichtigste Unterschied zu pgp/gpg ist wohl: Hier kannst du dein Zertifikat nicht einfach selbst ausstellen. Sinn ergibt das ganze nur, wenn es eine übergeordnete Stelle gibt, die Zertifikate ausstellt und der alle anderen vertrauen. Es handelt sich also um ein hierarchisches Modell im Gegensatz zum „Web of Trust“ (Netz des Vertrauens) von pgp/gpg.

Vorteile:

Nachteile:

- zentralisiert. Es gibt eine Instanz, der vertraut werden muss.