Robert Räke 15.12.2008

# PGP mit Thunderbird Mail (Windows)

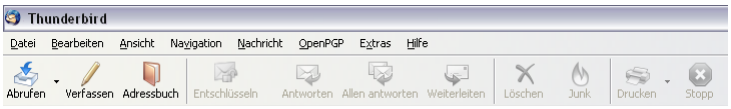
In dem Jahr 2008 wurde anhand einiger Vorkommnisse mal wieder deutlich, dass auch große Unternehmen nicht immer in der Lage sind, die Daten ihrer Kunden zu schützen. Hierbei handelt es sich nicht unbedingt um Hacker, welche sich Zugang zu der EDV einer Firma verschaffen, sondern vielmehr um Innentäter. Mitarbeiter, die unsere Daten sammeln und an Interessenten verkaufen.

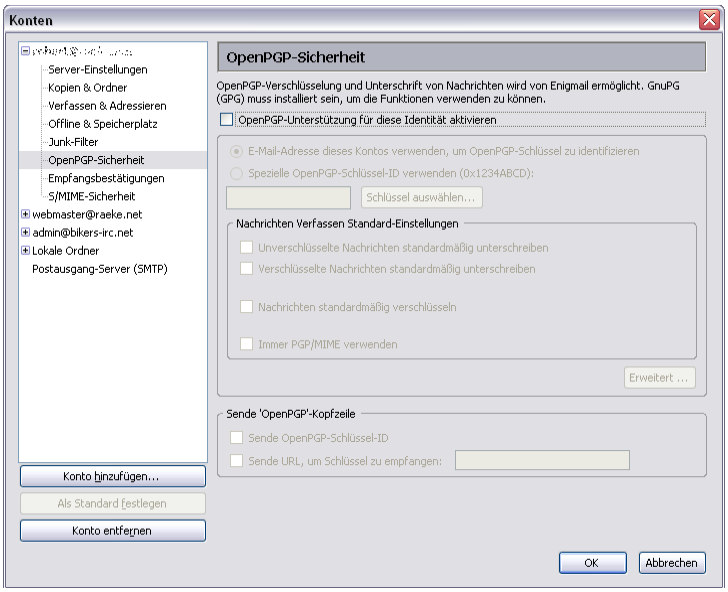
Sicher ist auf jedem Fall, dass ein großer Personenkreis Zugang zu unseren Daten hat. Dieses gilt jedoch nicht nur für Daten wie Vorname, Nachname, Geburtsdatum, etc., die wir zum Beispiel bei einem Vertragsabschluss angeben, sondern auch für unseren elektronischen Daten, die wir täglich austauschen.

Denn wo verbleibt denn eine von uns versendete e-Mail solange, bis der Empfänger sie von dem Server löscht? Sie bleibt auf dem Server unseres Internet-Providers liegen. Stellt sich nun die Frage, wie viele Administratoren, Support- und sonstige Mitarbeiter des Providers die Möglichkeit haben, unsere versendete e-Mail zu öffnen und zu lesen. Wem wird bei diesem Gedanken nicht etwas mulmig?

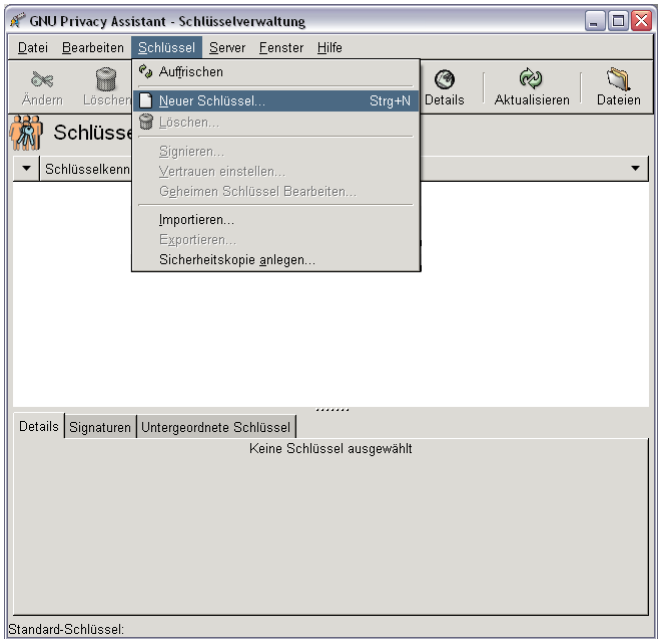
Wie kann ich also meine e-Mails so schützen, dass nur der Empfänger, für den die e-Mail bestimmt ist, diese lesen kann? Die Frage ist natürlich immer: „Gibt es den absoluten Schutz?“ Wohl nicht, aber wenn sich schon jemand an unseren Daten zu schaffen macht, wollen wir es ihm doch wenigstens so schwer wie möglich machen, diese einzusehen! Dabei hilft uns PGP (Pretty Good Privacy). Und die Verwendung ist nicht einmal schwer oder kompliziert. Auf die Grundlagen von PGP werde ich hier jedoch nicht eingehen. Darüber gibt es genug Informationen im Internet. Google oder Wikipedia helfen da sicher weiter. Dieses Dokument ist lediglich eine Anleitung zur Einrichtung von PGP unter Thunderbird Mail unter Windows. Die gesamte Software, die hier beschrieben ist, ist kostenlos und wird durch Spenden finanziert.

Als erstes benötigen wir natürlich unseren e-Mail Client **Thunderbird Mail**, zu dem wir die Erweiterung **Enigmail** installieren. Nach dem Neustart von Thunderbird Mail erhalten wir ein neues Drop-Down-Menü „OpenPGP“, einen Button „Entschlüsseln“ und zusätzliche Einstellungen „OpenPGP-Sicherheit“ in den Eigenschaften unserer eingerichteten e-Mail-Konten. Zur Konfiguration dieser Erweiterung kommen wir später.



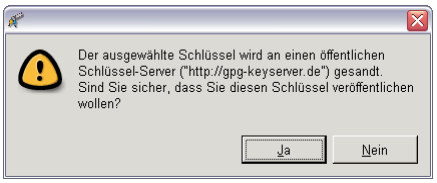



# PGP mit Thunderbird Mail (Windows)




Als nächstes laden wir **GnuPG für Windows** herunter und installieren dieses. Das Tool ist recht übersichtlich und somit kommen wir auch mit dem „GNU Privacy Assistant“ (GPA) schnell an unser Ziel:
In dem Drop-Down-Menü „Schlüssel“ wählen wir „Neuer Schlüssel...“ aus. Wir werden aufgefordert, den (vollständigen) Namen, e-Mail-Adresse und ein Passwortsatz einzugeben. Besonders ist bei dem Passwortsatz darauf zu achten, dass möglichst Groß- und Kleinschreibung sowie Zahlen und Sonderzeichen Verwendung findet. Auch sollte dieser Passwortsatz nicht nur Wörter enthalten, die in der gewählten Schreibweise auch in einem Wörterbuch zu finden sind. Genauso wenig sollten Daten verwendet werden, die leicht zu erraten sind, aber leider für die Verwendung bei Passwörtern sehr beliebt sind. Dazu gehören Geburtsdaten oder Namen von Angehörigen! Auch die Kombination dieser macht den Passwortsatz nicht sicherer!
Ohne diesen Passwortsatz ist der erzeugte Schlüssel jedoch wertlos! Ohne ihn auf dem Computer zu speichern, sollten wir ihn uns demnach trotzdem leicht merken können. Weitere Hinweise hierzu geben die PDF-Dokumente, die optional mit der Software installiert werden können.
Wer möchte, kann nach der Erstellung des Schlüssels diesem auch noch ein Verfallsdatum geben.

Nachdem wir unseren Schlüssel, der aus einem öffentlichem und einem geheimen Teil besteht, erstellt haben, macht es Sinn, den öffentlichen Schlüssel auch zu veröffentlichen. Den mit diesem Schlüssel wird eine e-Mail vom Absender verschlüsselt, wenn er sie an uns verschickt. Alternativ kann ich den öffentlichen Schlüssel auch an alle verschicken, mit denen ich per e-Mail kommuniziere, oder ich veröffentliche diesen auf der eigenen Homepage.
Es gibt auch Schlüsselserver, über die öffentliche Schlüssel abgefragt werden können. Möchte ich meinen Schlüssel dort veröffentlichen, so geht dieses über das Drop-Down-Menü „Server“ und der Auswahl „Schlüssel verschicken...“. Mehr auch hierzu in den PDF-Dokumenten der Software.



Wir haben nun unsere Schlüssel erstellt, schließen diese Anwendung und wechseln wieder zu Thunderbird Mail.

In dem Drop-Down-Menü „OpenPGP“ finden wir nun schon unter der Auswahl „Schlüssel verwalten...“ unseren erstellten Schlüssel wieder. Über den Kontext-Menüpunkt des Schlüssels „Benutzer-IDs verwalten...“ kann ich nun den Schlüssel auch noch anderen e-Mail-Adressen zuweisen.
Bleiben nur noch die Einstellungen „OpenPGP Sicherheit“ in den e-Mail-Konten:
Die OpenPGP-Unterstützung ist natürlich zu aktivieren. Die restlichen Einstellungen sind optional.

**Es bleibt noch ein wichtiger Hinweis:**
Der erstellte Schlüssel mit dem geheimen Teil sollte nicht sorglos auf der Festplatte liegen gelassen werden. Es empfiehlt sich, den Schüssel auf einer CD zu archivieren und diese zu verschließen.

**Versenden von verschlüsselten e-Mails:**
Wenn ich nun eine e-Mail verschlüsselt senden möchte, benötige ich den öffentlichen Schlüssel des Empfängers. Das suchen von öffentlichen Schlüsseln ist direkt über die Schlüssel-Verwaltung von Thunderbird Mail zu empfehlen, da hier zur Suche eine e-Mail-Adresse eingegeben werden kann. Ist ein öffentlicher Schlüssel zu dieser Adresse auf dem Key-Server vorhanden, wird dieser angezeigt. Nach der Auswahl wird auch dieser Schlüssel in unserer Schlüsselverwaltung angezeigt. Über das Kontext-Menü des Schlüssels „Besitzer-Vertrauen festlegen...“ müssen wir nun noch festlegen, wie sehr wir diesem Schlüssel vertrauen.
Mehr auch hierzu wieder in den PDF-Dokumenten der Software.

**Signieren von e-Mails:**
Wer sagt uns eigentlich, dass die e-Mail, welche in unserem Posteingang liegt, wirklich von dem uns bekannten Absender ist? Immer häufiger machen uns anonyme Mails mit gefälschten Absendern das Leben schwer. Würden Firmen digitale Signaturen bei E-Mails benutzen, wäre dem Phishing nahezu das Handwerk gelegt.
Auch hier haben wir durch unseren erstellten Schlüssel neue Möglichkeiten, denn mit diesem können wir unsere e-Mails mit einer digitalen Signatur versehen. Auf diese Weise ist für den Empfänger sichergestellt, dass diese Mail erstens von uns stammt und zweitens nach dem Versenden nicht durch jemanden verändert wurde.

Und nun viel Spaß beim sorglosen versenden von e-Mails!

**Software-Quellen:**

| | |
|---|---|
| Thunderbird Mail: | http://www.thunderbird-mail.de/ |
| Enigmail: | http://www.erweiterungen.de/detail/Enigmail/ |
| GnuPG für Windows: | http://www.gpg4win.de/ |