Würden Sie ihre vertrauliche Korrespondenz mit Ämtern, Geschäftspartnern und Freunden im traditionellen Briefverkehr als Postkarte verschicken? Sicher nicht, schließlich möchten Sie ja nicht, dass der Briefträger und jeder Sortierer bei der Post ihre Korrespondenz mitliest. Wenn Sie jedoch elektronische Post, also E-Mails, verschicken, dann verschicken Sie in der Regel elektronische Postkarten, die nicht nur neugierige Geheimdienste und Internetdienstleister, sondern mit überschaubarem Aufwand auch jeder kleine Hacker mitlesen kann. Als Abhilfe bietet sich hier vor allem der Versand und Empfang von verschlüsselten Mails an. Die Ersteinrichtung der dafür benötigten Software ist zwar für Computerlaien nicht ganz so einfach. Es gibt jedoch zahlreiche Tutorials im Netz, mit denen Sie mühelos den Einstieg in die Welt der Verschlüsselung meistern sollten. Von **Jens Berger**.

Warum sollte man Mails überhaupt verschlüsseln?

Für Personen, die – auf welche Weise auch immer – mit wirklich vertraulichen und sensiblen Daten zu tun haben, ist eine Verschlüsselung der übermittelten Daten zwingend angeraten. Dazu gehören neben Anwälten, Ärzten, Steuerberatern und jeglichen Personen, die in einem beruflichen Umfeld tätig sind, in dem sie Zugriff auf Daten haben, die für die Konkurrenz von Interesse sein könnten, vor allem auch Journalisten. Erstaunlich und höchst ärgerlich ist, dass vor allem die Journalisten beim Thema „Verschlüsselung“ offenbar nicht das geringste Problembewusstsein aufweisen. Dieser kleine Service-Artikel ist jedoch nicht für diese Personengruppen gedacht und geeignet! Denn was nützt die beste Verschlüsselung, wenn die Person, um die es geht, anderweitige Sicherheitslecks hat. Wenn Ihr Windows-Betriebssystem beispielsweise von Trojanern oder anderen Schadprogrammen infiziert ist[*], können auch verschlüsselte Mails mitgelesen werden. Mehr noch, Verschlüsselung in kompromittierter Umgebung kann sogar mehr schaden als nützen, weil es dem Empfänger Ihrer oder in Ihren Namen gefälschten Nachrichten ein falsches Sicherheitsgefühl vermittelt.

Wer zu den genannten Personengruppen gehört und eine Arbeitsumgebung nutzt, die generell als unsicher zu gelten hat (und dazu zählt grundsätzlich das Betriebssystem Windows), sollte daher auch einen Profi konsultieren, der das System – so gut es geht – absichern kann.

Anders stellt es sich für Privatpersonen und Menschen in einem weniger sensiblen beruflichen Umfeld dar. Leider ist gerade bei dieser Gruppe jedoch die Fehleinschätzung weit verbreitet, dass Sie durch zusätzliche Sicherheit nichts zu gewinnen hätten. Wer nichts zu verbergen hat, muss auch nichts verschlüsseln. Ist dem so? Stellen Sie sich doch einmal folgende Situation vor: Sie sitzen in einem Straßencafé und ihr Smartphone ruft über einem

vom Cafébetreiber freundlicherweise installierten W-Lan-Hotspot der Telekom automatisch ihre Mails ab. Sollte die Verbindung zu ihrem Mail-Account nicht so konfiguriert sein, dass sie automatisch verschlüsselt ist, kann ein Hacker mit simplen Tools nicht nur ihre Mails mitlesen, sondern auch ihre Account-Daten (Nutzername und Passwort) abfangen[**] und auch in Zukunft ihre Mails mitlesen und Mails in ihrem Namen verschicken. Ein solcher „Hacker" muss dabei keinesfalls besonders talentiert sein. In den einschlägigen Foren gibt es für solche Zwecke auch Software, die sich über eine einfache Benutzeroberfläche von jedem bedienen lässt, der zumindest die Grundzüge der Netzwerktechnik beherrscht.

Abhilfe Verschlüsselung – Grundlagen der Technik

Wenn es hier um die Verschlüsselung von Mails geht, dann geht es ausschließlich um die Verschlüsselung des Inhaltes von E-Mails vom Absender bis zum Empfänger. Es geht nicht um die verschlüsselte Verbindung zu Ihrem Mail-Account (TLS/SSL), die „lediglich" dafür sorgt, dass die Kommunikation zum Mailserver selbst verschlüsselt wird. Für talentierte Hacker ist diese Verschlüsselung jedoch angreifbar und es ist zu vermuten, dass die Geheimdienste ohnehin Zugriff auf die unverschlüsselten Rohdaten haben – dass gilt erst Recht für die Internetdienstleister selbst.

Wenn wir heute von verschlüsselten Mails sprechen, dann geht es dabei in aller Regel um Verschlüsselung der Nachrichten, also des Inhalts von E-Mails, wofür sogenannte „asymmetrische" und „hybride" Verschlüsselungsverfahren eingesetzt werden. Ein „symmetrisches" Verschlüsselungsverfahren, das mit dem Schloss einer Tür vergleichbar ist, für das es einen Schlüssel zum ab- und aufschließen gibt, hat nämlich den entscheidenden Nachteil, dass es nur einen Schlüssel gibt, der in diesem Falle gesichert zum Empfänger übermittelt werden müsste. Bei einem asymmetrischen Verfahren, das mit einem Schlüsselpaar aus einem geheimen (privaten) Schüssel und einem öffentlichen Schüssel arbeitet, gibt es diesen Nachteil nicht. Die technischen Details sollten an dieser Stelle nicht weiter ausgeführt werden – technisch Interessierte finden dazu im Netz Informationen zuhauf. Die Grundlagen des Mailversands mit asymmetrischen Schlüsseln, sind jedoch vor allem für Einsteiger sehr wichtig.

Privater Schlüssel und öffentlicher Schlüssel – der Versand von verschlüsselten Mails

Wenn Sie sich mit Hilfe der weiter unten aufgeführten Software einen „Schüssel" erstellen lassen, so bekommen Sie mindestens zwei Schlüssel in einem Schlüsselpaar zu Verfügung gestellt – einen geheimen (privaten) Schüssel und einen öffentlichen Schlüssel. Die eigentliche Verschlüsselung erfolgt dabei stets in einer mathematisch komplizierten

Kombination aus dem geheimen Schlüssel des Absenders und dem öffentlichen Schlüssel des Empfängers.

Dieser öffentliche Schlüssel ist in der Tat „öffentlich“, Sie können (und sollten) diesen Schüssel allen Interessierten zur Verfügung stellen. Mein öffentlicher Schlüssel (für jb(at)nachdenkseiten.de) hat beispielsweise die **ID-Nummer** 50153232E999A2B5 und kann unter Eingabe dieser Nummer von jedem Open-PGP-Schlüsselserver abgerufen werden. Wenn Sie an die Redaktion der NachDenkSeiten (redaktion(at)nachdenkseiten.de) schreiben wollen, nutzen Sie bitte den Schlüssel mit der **ID-Nummer** 4A1E41373306C7E4. Für unsere Hinweisadresse gibt es keinen Schlüssel, da es sich hierbei um einen Verteiler handelt. Da in Theorie und Praxis jedoch auch „böse Buben“ einen Schlüssel für die Mail-Adressen der NachDenkSeiten erstellen und auf einen öffentlichen Schlüsselserver hochladen können, ist es im Zweifelsfalle auch wichtig, sich von der Korrektheit der Schlüssel überzeugen. Der zum Schlüssel gehörende „**Fingerabdruck**“ schafft hier die nötige Sicherheit. Der **Fingerabdruck** zum Schlüssel jb(at)nachdenkseiten.de lautet 104F F5AD 2CB1 E296 0646 39F8 5015 3232 E999 A2B5, der **Fingerabdruck** für den Schlüssel redaktion(at)nachdenkseiten.de A981 19E4 F71B 829B D24C 16ED 4A1E 4137 3306 C7E4. Sie finden diese Angaben übrigens auch in unserem Impressum und auf unserer Kontaktseite.

Neben der Verschlüsselung ist auch die Signatur von Mails eine Grundfunktion der asymmetrischen Verschlüsselung. Bei der Signatur von Mails wird stets der öffentliche Schlüssel mitgeschickt und anhand von Algorithmen mit der Absenderadresse verglichen. Wenn Sie also von mir eine signierte Mail erhalten und auch der Fingerabdruck des Schlüssels übereinstimmt, können Sie zumindest sicher sein, dass die Mail von meinem Rechner verschickt wurde und nebenbei haben Sie dann auch schon meinen öffentlichen Schüssel, um mir eine verschlüsselte Mail schicken zu können. Sobald Sie in ihrem Mailproramm eine Empfänger-Adresse eingeben, für die ihr Verschlüsselungsprogramm einen öffentlichen Schlüssel hat, wird bei Ihnen auch das Feld „Verschlüsseln“ freigegeben.

Wenn Sie eine verschlüsselte Mail an einen unbekannten Empfänger oder einen Empfänger, dessen öffentlichen Schlüssel Sie nicht besitzen, versenden wollen, hilft zunächst einmal die Abfrage bei einem der Open-PGP-Schlüsselserver, die über die hier genannte Software spielend leicht über die Eingabe der Mail-Adresse des Empfängers vonstatten geht. Sollte Ihr Empfänger dort nicht gelistet sein, so können Sie ihn über eine unverschlüsselte (aber wenn möglich signierte) Mail bitten, Ihnen den öffentlichen Schlüssel zu schicken und Ihnen – wenn möglich – den Fingerabdruck des Schlüssels über Telefon mitzuteilen. Ein potentieller Hacker kann diesen öffentlichen Schlüssel ruhig abfangen, da er mit ihm so lange nichts anfangen kann, bis er nicht auch den geheimen Schlüssel hat.

Sicherheitsmaßnahmen

Anders als den öffentlichen Schlüssel sollten Sie den geheimen Schlüssel daher auch wirklich geheim halten und eine Sicherungskopie des geheimen Schlüssels nach besten Möglichkeiten verstecken. Sie könnten ihn beispielweise auf einem USB-Stick speichern und den Stick an einem wirklich sicheren Ort (z.B. einen Bankschließfach oder zumindest einer abschließbaren Kassette) verwahren. Wichtig ist hier vor allem aber, dass sie eine Kopie erstellen, die sie separat von ihrem Computer hinterlegen. Sollten Sie nämlich einmal nicht mehr auf ihre Systemfestplatte zurückgreifen können (Diebstahl, Festplattenfehler, Feuer o.ä.), dann könnten Sie ohne Kopie ihres privaten Schlüssels nicht mehr auf verschlüsselte Mails zurückgreifen, selbst wenn diese separat auf einem anderen Rechner gespeichert sind. Sollte Ihnen einmal Ihr Rechner entwendet werden, können Sie den alten Schlüssel übrigens über ein sogenanntes Rückruf-Zertifikat ungültig machen und sich ein neues Schlüsselpaar ausstellen lassen. Dafür sollten Sie jedoch auch das Rückruf-Zertifikat (z.B. zusammen mit der Kopie des privaten Schlüssels) separat vom Computer hinterlegen.

Als zusätzlichen Schutz gibt es zudem die sogenannte „Passphrase“, die Sie jedes Mal benötigen, wenn ihr Rechner auf den Privatschlüssel zugreifen will. Wählen Sie am besten ein Passwort, das Sie auch garantiert nicht vergessen und dass sie auf keinen Fall an anderer Stelle, die von Hacken kompromittiert werden könnte, auch nutzen – z.B. für den Mail-Account. Es ist ratsam, dass Sie diese Passphrase ebenfalls separat vom Rechner notieren und verwahren – ansonsten kann es Ihnen nämlich passieren, dass Sie sich selbst aussperren. Und da die Verschlüsselungsmechanismen sehr sicher sind, gibt es auch weder eine Hintertür, einen Zweitschlüssel noch die Möglichkeit, einen Schlüsseldienst zu bestellen.

S/MIME und (Open)PGP – zwei inkompatible Standards

Wie so oft machen es die Softwareanbieter den Nutzern auch beim Thema Verschlüsselung unnötig schwer, da es zwei weit verbreitete miteinander konkurrierende Verschlüsselungsmechanismen gibt, die zudem nicht miteinander kompatibel sind – S/MIME und (Open)PGP. Ohne nun auf die technischen Details einzugehen, lässt sich hier zusammenfassen, dass die Unterschiede dieser beider Standards nicht in der Verschlüsselung selbst, sondern in der Signierung/Zertifizierung liegen. Während S/MIME hier auf zentrale hierarchische Zertifikate setzt, die durch dafür zertifizierte Stellen ausgegeben wurden, setzt Open PGP auf ein sogenanntes Web of Trust, bei dem sich die Nutzer selbst beglaubigen. S/MIME erlaubt jedoch keine anonyme Nutzung und ist daher beispielweise für Whistleblower uninteressant. Da S/MIME zudem ein absolutes Vertrauen in die Zertifizierungsstelle voraussetzt, kann man dieses Verfahren auch nicht mit gutem

Gewissen empfehlen. Oder kennen Sie Unternehmen wie Start Commercial Limited, GMO Globalsign Limited oder VeriSign Incorporated und deren jeweilige Hintermänner so gut, dass Sie diesen Unternehmen blindlings absolut vertrauen würden? Daher beschränken wir uns hier auch auf die Darstellung von Open PGP. Sollten Sie Interesse an S/MIME haben, sollten Sie sich an einen Profi wenden, der Ihnen diesen Standard erklärt und Ihr System fit dafür macht.

Installation der passenden Software

Passende und zudem kostenlose Softwarelösungen, die sowohl leicht zu installieren, wie zu bedienen sind, gibt es für alle verbreiteten Computerbetriebssysteme. Schlechter sieht es da bei den Smartphones aus. Im Folgenden will ich Ihnen einen kurzen Einblick in die gängigsten Programmvarianten geben:

1. **Betriebssystem Windows und Mozilla Thunderbird**

   Für das populäre, aber aus Sicherheitsgesichtspunkten wohl gefährlichste, Betriebssystem Windows (XP, 7 oder 8) gibt es zahlreiche Softwarelösungen, mit denen man in Kombination mit den weit verbreiteten Mail-Programmen seinen Mail-Verkehr wirkungsvoll verschlüsseln kann. Eine Ausnahme bildet hier die keineswegs seltene Kombination des Microsoft-Betriebssystems mit dem Microsoft-Mailprogramm Outlook. Mir persönlich ist hier kein kostenloses Programm/Plugin bekannt, das Open PGP in sämtlichen aktuellen Versionen von Outlook implementieren könnte[***]. Eine kostenpflichtige Softwarelösung ist gpg4o vom deutschen Hersteller Giegerich & Partner. Da ich diese Software jedoch nicht nutze, kann ich an dieser Stelle auch keine Empfehlung aussprechen.

   Empfehlenswert ist jedoch ohne Zweifel die (Parallel-)Nutzung des populären Open-Source-Programms Thunderbird, für das kostenlose Plugins zur sicheren Mailverschlüsselung zur Verfügung stehen. Freilich können Sie Thunderbird auch als „Zweitprogramm“ neben Outlook nutzen – dann sollten Sie jedoch darauf dachten, dass die Mails bei einem genutzten POP-Account nicht vom Server gelöscht werden. Wenn Sie jedoch nicht an Outlook hängen, ist ein Umstieg auf Thunderbird auch abseits der Verschlüsselungsthematik zu empfehlen.

   Als Grundlage für die Verschlüsselung von Mails benötigen Sie dabei das kostenlose Programm Gpg4win, mit dem Sie ihre Schlüssel erstellen und verwalten können. Gpg4win beinhaltet auch ein Plugin für ältere Outlook-Versionen – neuere Versionen (ab Outlook 2010) werden jedoch nicht unterstützt. Bei der eigentlichen Mailver- und

entschlüsselung werkelt Gpg4win im Hintergrund. Wenn Sie Mails über Thunderbird ver- und entschlüsseln wollen, müssen Sie daher noch die dafür nötige Benutzeroberfläche, die über das ebenfalls kostenlose Thunderbird-Plugin Enigmail bereitgestellt wird.

Zur Installation und Bedienung der Softwarekombination Windows/Thunderbird/Gpg4win/Enigmal gibt es im Netz zahlreiche gute Tutorials und Einführungen. Drei Tutorials seien an dieser Stelle für Einsteiger besonders empfohlen:

- Burkhard Schröder (burks) – E-Mails verschlüsseln in 30 Minuten
- Rainer Klute – Sichere E-Mail-Kommunikation mit OpenPGP
- Verbraucher-Sicher-Online – E-Mails verschlüsseln in Mozilla Thunderbird mit Enigmail und Gnu Privacy Guard

2. **Betriebssystem Mac OS X und Apple Mail**

   Noch einfacher gestaltet sich die Sache, wenn man Mac OS X und Apples bordeigenes Mail-Programm benutzt. In dieser Kombination sind die kostenlosen GPGTools zu empfehlen. Das Installationsprogramm installiert neben der Verwaltungssoftware „GPG Schlüsselbund“ gleich auch das passende Plugin für Apple Mail mit. Hilfreiche deutsche Tutorials sind u.a. auf den Seiten Verbraucher-Sicher-Online und dem Blog macon.cc zu finden und auch das Tutorial von GPGTools selbst ist sehr empfehlenswert, aber leider (bislang) nur in englischer Sprache verfügbar. . Da ich selbst diese Kombination nutze, können Sie Fragen dazu auch gerne per Mail an jb(at)nachdenkseiten.de schicken.

   Wer unter Mac OS das Mailprogramm Thunderbird nutzt, kann übrigens ebenfalls das unter Windows verlinkte Plugin Enigmail nutzen – dann ist jedoch statt Gpg4win die Installation der GPGTools nowendig.

3. **Linux**

   Anders als Windows und Mac OS X bringen die meisten Linux-Distributionen die grundlegende Software zur Ver- und Entschlüsselung von Mails bereits von Haus aus mit. Wie man das Thunderbird-Plugin Enigmail unter Linux installiert, zeigen zahlreiche Linux-Nutzerforen – u.a. hier. Da ich persönlich kein Linux nutze und davon

überzeugt bin, dass Linux-Nutzer sich mit ihrem System ohnehin so gut auskennen, dass sie keine Einsteigertipps benötigen, sehe ich mich auch nicht in der Lage hier Tipps oder gar Empfehlungen auszusprechen. Wer Einsteigertipps sucht, sollte sie ohne Probleme in der gut aufgestellten Linux-Community finden.

4. **Webmail**

   Die unter (1) bis (3) aufgeführten Software-Lösungen sind für „echte“ Mailprogramme konzipiert, die mit dem Mailserver über POP oder IMAP kommunizieren. Viele Nutzer bevorzugen jedoch stattdessen lieber die meist kostenfreien Webmail-Dienste diverser Anbieter wie z.B. GMX, Google, Yahoo oder Web.de. Für Nutzer dieser Dienste gibt es die Software „Mailvelope“, die es kostenlos als Plugin für die Browser Firefox und Google Chrome gibt. Mit dieser Lösung lässt sich über die Dienste Googlemail, Yahoo Mail, Outlook.com und GMX die Open-PGP-Verschlüsselung über den Browser selbst nutzen. Das funktioniert zwar, man sollte sich jedoch die Frage stellen, ob es ratsam ist, derart sensible Informationen der Plugin-Verwaltung eines Internetbrowsers anzuvertrauen – zumal, wenn es sich wie bei Google Chrome um ein Produkt des Hauses Google handelt. Daher sollten sich die Nutzer auch über mögliche Sicherheitslecks im Klaren sein, weshalb hier keine Empfehlung für eine derartige Lösung abgegeben werden soll.

   Unbedingt meiden sollten Sie übrigens „Verschlüsselungsdienste“, die Ihnen von Ihrem Webmail-Anbieter gestellt werden. Bei diesen Diensten wird Ihr privater Schlüssel vom jeweiligen Anbieter gespeichert und verwaltet – das ist so ziemlich das exakte Gegenteil von Sicherheit.

5. **Smartphones**

   Dies gilt umso mehr für die Nutzung von Verschlüsselungssoftware auf Smartphones. Es werden zwar für sämtliche gängigen Smartphone-Betriebssysteme (iOS, Android und Windows Phone) diverse Apps angeboten, mit denen man eine Open-PGP-Verschlüsselung der Mails handhaben kann. Eine solche Verschlüsselung kann jedoch stets nur so sicher und vertrauensvoll sein wie das Betriebssystem selbst. Und es ist ja bekannt, dass alle hier genannten Betriebssysteme nur zu gerne „nach Hause funken“ und sämtliche Informationen an die Herstellerfirmen Apple (iOS), Google (Android) und Microsoft (Windows Phone) weiterleiten – Unternehmen, die überdies Bestandteil des Prism-Programms sind. Da ich generell an der Sicherheit dieser Systeme zweifele, halte ich es auch für nicht für sinnvoll, diesen Systemen sensible Daten anzuvertrauen und der private Schlüssel ist sehr sensibel und sollte ganz sicher nicht in die Hände

derartiger Unternehmen geraten***. Daher sollte man seine Mails auch wenn möglich nicht über das Smartphone ver- und entschlüsseln. Die meisten Mails sind schließlich auch nicht so dringend, dass man mit der Ver- und Entschlüsselung nicht so lange warten kann, bis man Zugriff auf seinen Desktop- oder Laptop-Rechner hat.

Sicherheitsplus aber keine Sicherheitsgarantie

Wer seine Mails nach den hier genannten Verfahren verschlüsselt, ist zunächst einmal auf der sicheren Seite. Nach allen bekannten Informationen ist es selbst für die NSA nicht möglich, Nachrichten, die mit moderner asymmetrischer Verschlüsselung verschlüsselt wurden, in einem vertretbaren Zeitrahmen zu entschlüsseln. Eine Sicherheitsgarantie ist dies jedoch nicht! Jede Ver- und Entschlüsselung ist nur so sicher, wie das System, mit dem sie ver- und entschlüsselt wird. Und wenn Sie beispielsweise über einen vollkommen unsicheres Windows-System ins Netz gehen, bei dem z.B. wegen „ungeklärter Lizenzfragen“ die Update-Funktion deaktiviert ist, sollten Sie sich vor allem darüber im Klaren sein, dass ihr Rechner für Schadsoftware offen wie ein Scheunentor ist. Wenn Sie dann auch noch gerne über öffentliche Hotspots ins Netz gehen, sind Sie ohnehin ein gefundenes Fressen für Hacker und „Script-Kiddies“. Bildlich gesprochen, hätten Sie dann ihre Eingangstür mittels Open PGP nach dem sichersten aller Standards verrammelt, gleich nebenan sind die jedoch die morschen Holzfenster in ihrer Abwesenheit sperrangelweit offen. Dies ist nicht nur für Sie ein Risiko, sondern auch für sämtliche Personen, die mit Ihnen vertraulich kommunizieren.

Die Verschlüsselung von Mails ist ein wichtiger Baustein für die Sicherheit von Informationen. Mehr als ein Baustein ist sie jedoch nicht. In folgenden Artikeln werden wie Ihnen jedoch auch gerne noch Tipps geben, wie Sie ihr Computersystem auch ansonsten halbwegs sicher halten. Eine totale Sicherheit ist übrigens nach normalen Standards nicht möglich – außer Sie arbeiten auf zwei Systemen, eines mit Internetzugang und eines ohne offene Netzwerkverbindungen für die sensiblen Daten; im Hochsicherheitsbereich von Unternehmen und Organisationen ist dies übrigens keinesfalls selten. Im Privatbereich ist so etwas jedoch meist nicht sinnvoll zu realisieren. Daher sollte für Sie als Privatanwender auch die goldene Regel gelten, dass Informationen generell unsicher sind. Mit den hier vorgestellten Maßnahmen können Sie die Unsicherheit lediglich reduzieren – nicht mehr, aber auch nicht weniger.

[«*] Für eine solche Infektion reicht es oft bereits, ein bestimmte Internetseite aufzurufen,

die über sogenannte Injections (z.B. über Java und Javascript) Softwaremodule auf Ihrem Rechner installiert.

[«**] Mittels ARP-Spoofing und sogenannten Man-in-the-middle-Angriffen können Hacker auch ihre Account-Daten zu sozialen Netzwerken und – wenn Sie etwas talentierter sind – auch via SSL verschlüsselte Mail-Accounts auslesen und manipulieren. Ein Kapern des PayPal-Kontos ist damit ein Kinderspiel.

[«***] Sollten Sie sich auf diesem Gebiet besser auskennen und Tipps für uns und unsere Leser haben, scheuen Sie sich nicht, uns per Mail Informationen zu geben. Wir werden diese Informationen dann in den Hinweisen des Tages nachtragen.