Sebastian Schreiber

Mut zur Verschlüsselung

Kaum ein Tag vergeht, an dem wir nicht in der Tagespresse von Hackerangriffen oder Spionagetätigkeiten wie das Auslesen von E-Mails lesen. Dabei gibt es schon seit Jahren Möglichkeiten, den Nachrichtenverkehr zu verschlüsseln. Um verschlüsselt kommunizieren zu können, muss eine Verschlüsselungstechnik sowohl auf dem eigenen Rechner als auch auf Rechnern der jeweiligen E-Mail-Kontakte installiert werden.

An Verschlüsselungsverfahren und Möglichkeiten, eine E-Mail-Verschlüsselung auf dem eigenen Rechner umzusetzen, mangelt es nicht. Doch keine noch so ausgefeilte und reibungslos laufende Verschlüsselungstechnik schützt vor dem ungewollten Mitlesen Dritter, wenn die eigenen Mailkontakte keine Verschlüsselungsverfahren einsetzen. Folgendes ist deshalb ratsam:

1. Implementieren Sie bei sich eine E-Mail-Verschlüsselung.
2. Ermuntern Sie Ihre Geschäfts- und Privatkontakte, mit Ihnen verschlüsselt zu kommunizieren, und verteilen Sie Ihren öffentlichen Schlüssel.
3. Helfen Sie sich gegenseitig, Hemmungen vor Verschlüsselungsprogrammen abzubauen. Sicherlich muss man sich in jede neue Technik eindenken und vielleicht funktioniert auch nicht immer alles sofort. Dennoch lohnt es sich, die Möglichkeiten zur Verschlüsselung von E-Mails wahrzunehmen.
4. Nutzen Sie das Netz, um Hilfe bei der Installation Ihrer Verschlüsselungsprogramme zu bekommen. Es gibt eine Reihe von Webseiten, die Ihnen anschaulich erklären, wie Sie auf Ihrem Betriebssystem eine Verschlüsselung bei Ihrem E-Mail-Programm einrichten können.
5. Falls eine Ende-zu-Ende-Verschlüsselung nicht möglich ist, können vertrauliche Daten auch als passwortgeschützte ZIP-Dateien versandt werden: Intern werden die Dateien dann mit einem aus dem Passwort generierten Schlüssel verschlüsselt.

Die sicherste Möglichkeit, Daten vertraulich zu übermitteln ist, eine Ende-zu-Ende-Verschlüsselung *(End-to-End Encryption)*. Dabei verschlüsselt der Absender die Nachricht, die Übertragung erfolgt lückenlos verschlüsselt und der Empfänger entschlüsselt die Nachricht dann. Das Prinzip ist klar, doch wie können selbst technisch nicht besonders versierte Computernutzer eine solche Verschlüsselung beispielsweise für E-Mails bei sich auf ihrem Rechner umsetzen?

Dieser Artikel wird in erster Linie auf das PGP-Verfahren eingehen, weil es im Gegensatz zu S/MIME kostenlos ist und sich für jeden privaten Computernutzer eignet, doch auch S/MIME soll zum Schluss kurz beschrieben werden. Ebenso beschränkt sich der Artikel auf die E-Mail-Verschlüsselung auf Rechnern, wobei es freilich auch die Möglichkeit gibt, PGP, S/MIME oder andere Verfahren zum Beispiel auch auf Smartphones einzusetzen.

OpenPGP

Um E-Mails verschlüsseln zu können, bedarf es mehrerer Komponenten. Zum einen braucht ein User ein geeignetes Programm wie zum Beispiel Gpg4win, das ein Schlüsselpaar erzeugt, mit dem die E-Mail-Kommunikation ver- und entschlüsselt werden kann.

Dieses Paar besteht aus einem öffentlichen und einem privaten Schlüssel *(Public/Private Key)*. Der User verteilt seinen öffentlichen Schlüssel an seine Mailkontakte oder legt ihn auf öffentlich zugänglichen Key-Servern ab und erhält im Gegenzug die öffentlichen Schlüssel seiner Kontakte, die er bei sich in der Schlüsselverwaltung speichert. Jeder Schlüssel erzeugt einen sogenannten Fingerprint, welcher eine Kurzform des Schlüssels darstellt und dazu dient, öffentliche Schlüssel als zum Adressaten gehörend zu verifizieren. Um einen sicheren E-Mail-Austausch zu gewährleisten, sind Fingerprints so gestaltet, dass sie leicht auf unterschiedlichen Wegen ausgetauscht werden können, zum Beispiel auch mündlich oder per SMS. Auf diese Weise kann sichergestellt werden, dass – solten Zweifel bezüglich eines erhaltenen öffentlichen Schlüssels bestehen – Fingerprints über andere Kanäle verschickt werden als der Schlüssel selbst.

Wenn nun Tanja zum Beispiel Karin verschlüsselt schreiben will, verschlüsselt sie die Nachricht mit Karins öffentlichem Schlüssel, den sie bei sich in der Schlüsselverwaltung abgespeichert hat. Wenn Karin zurückschreibt, verschlüsselt sie mit Tanjas öffentlichem Schlüssel. Mit dem Fingerprint können beide die Echtheit des Absenders verifizieren.

Den privaten Schlüssel brauchen Tanja und Karin, um die empfangenen verschlüsselten E-Mails wieder zu entschlüsseln. Im Gegensatz zum öffentlichen Schlüssel sollte der private Schlüssel nie aus der Hand gegeben werden. Er hat einen hohen Schutzbedarf. Um zu verhindern, dass er durch Dritte ausgelesen wird, ist es ratsam, diesen Schlüssel mit einer hinreichend langen und komplexen Passphrase zu schützen.

Computernutzer, die Thunderbird als E-Mail-Programm nutzen, können die Verschlüsselung recht einfach umsetzen. Voraussetzung hierfür sind das Thunderbird-Add-On Enigmail und das Programm Gpg4win in der jeweils aktuellen Version.

Wenn alles installiert ist, kann begonnen werden, mit dem OpenPGP-Assistenten die eigene E-Mail-Verschlüsselung einzurichten. Dabei können Nutzer beispielsweise festlegen, alle ausgehenden E-Mails zu signieren. Dies ist zwar einer Verschlüsselung nicht ebenbürtig und schützt nicht vor einem etwaigen Mitlesen, aber der Absender verifiziert dadurch, dass er die E-Mail verfasst hat und beugt einem möglichen Missbrauch oder Fake-E-Mails vor.
Der Assistent erzeugt auch das zum Verschlüsseln notwendige Schlüsselpaar und fordert dazu auf, eine Passphrase einzugeben. Bei der Erzeugung eines Schlüsselpaars ist vor allem darauf zu achten, eine Widerrufserklärung einzurichten, damit der Schlüssel bei Verlust oder Datenklau ungültig gemacht und aus dem Verkehr gezogen werden kann. Der OpenPGP-Assistent fragt im Zuge der Schlüsselerzeugung automatisch ab, ob eine solche Erklärung eingerichtet werden soll. Eine Möglichkeit zum Widerruf ist insofern wichtig, da Schlüssel, die einmal auf Key-Server geladen werden, nicht mehr gelöscht werden können.

Nutzer von Outlook stellen die Verschlüsselung über das Programm Gpg4win ein. Dazu ist es wichtig, bei der Installation von Gpg4win darauf zu achten, die Komponenten Kleopatra und GpgOL auszuwählen und mitzuinstallieren. Wenn alles erfolgreich eingerichtet ist, muss das Programm Kleopatra geöffnet und dort unter

„Datei“ „Neues Zertifikat“ ausgewählt werden, um ein Schlüsselpaar zu erstellen. Die Installation erfolgt ähnlich wie bei Thunderbird; auch hier verlangt Kleopatra eine Passphrase für den privaten Schlüssel. Wenn Nutzer die öffentlichen Schlüssel ihrer Mailkontakte erhalten, so speichert Kleopatra diese in einer speziellen Zertifikatverwaltung. Diese wird dann mit Outlook verknüpft und für einen verschlüsselten E-Mail-Verkehr bereitgestellt.

Auch Apple-User haben die Möglichkeit, PGP zur Verschlüsselung von E-Mails zu verwenden. Dazu benötigen sie das Programm Mac GNU Privacy Guard, die freie Mac-Variante eines Kryptographiesystems, den GPG-Schlüsselbund, eine graphische Benutzeroberfläche zur Schlüsselverwaltung, und GPGMail, ein Plugin für Apple Mail für die Ver- und Entschlüsselung sowie fürs Signieren.

Nach der Installation von Mac GNU Privacy Guard kann über den GPG-Schlüsselbund ein Schlüsselpaar erstellt werden. Nutzer klicken hierfür auf „Neu“ und erzeugen das Paar über den Assistenten. Ein interessantes Detail: Bei Apple ist die Schlüssellänge oftmals mit 1024 Bit voreingestellt, der Nutzer kann aber diese Länge manuell auf 4096 erhöhen. Das ist empfehlenswert, wenn man den Schlüssel einige Jahre lang nutzen möchte. Ebenso fordert der Assistent den Nutzer auf, seinen privaten Schlüssel mit einer Passphrase zu schützen.

S/MIME

Obschon S/MIME Ähnlichkeiten zu OpenPGP aufweist, sind beide Verschlüsselungsverfahren nicht kompatibel. S/MIME verwendet zum Ver- und Entschlüsseln von E-Mails das Zertifikat einer vertrauenswürdigen Certification Authority (CA), welches wiederum die Authentizität des Absenders beglaubigt. Ein S/MIME-Zertifikat muss beantragt und gekauft werden, wobei auch Zertifizierungsstellen existieren, die Privatpersonen kostenlose Klasse1-Zertifikate anbieten. Wenn Antrag und Registrierung bei der CA erfolgreich waren, kann das Zertifikat in den Webbrowser exportiert und von dort in das jeweilige E-Mail-Programm importiert werden. Meist gibt es unter „Einstellungen“ oder „Erweiterte Einstellungen“ Stellen, wo solche Zertifikate abgelegt werden können. S/MIME wird gerne von Unternehmen genutzt, die Wert darauf legen, dass die Authentizität ihrer Kommunikationspartner verifiziert wird.

Mit der Anwendung einer E-Mail-Verschlüsselung gelingt es uns, unsere Privatsphäre immens gegen den Einblick Dritter zu schützen und etwas gegen die stetige Gefahr zu tun, ausgespäht zu werden.

Weiterführende Links

https://netzpolitik.org/2013/anleitung-so-verschlusselt-ihr-eure-e-mails-mit-pgp/
http://blog.dirkeinecke.de/2008/01/apple-mail-und-pgp.html
http://praxistipps.chip.de/outlook-e-mails-mit-pgp-verschluesseln_29276
http://www.heise.de/ct/artikel/Brief-mit-Siegel-1911842.html
http://cyber-security-blog.de/smime-mail-verschluesselung-signierung/#lb2c