RUBIKON

Donnerstag, 14. September 2017, 10:38 Uhr
~8 Minuten Lesezeit

E-Mail-Verschlüsselung ist sinnvoll und notwendig

Die Verschlüsselung von E-Mails ist Teil der digitalen Selbstverteidigung.

von Wolfgang Romey

Wie lange ist es eigentlich her, dass Edward Snowden mit seinen unglaublichen Enthüllungen an die Öffentlichkeit ging? Fünf Jahre, zehn Jahre? Am 20. Mai 2013 flog Snowden nach Hong Kong und danach war alles anders. Oder nicht? Was hat sich eigentlich verändert? Die Geheimdienste haben mehr Geld bekommen, ihre Aktivitäten sind teilweise legalisiert worden und sie machen nun mit Wissen der Öffentlichkeit weiter wie bisher. Was sich trotz der

anfänglichen großen Empörung (fast) nicht geändert hat, ist das Verhalten der Internet-Nutzer. Dabei ist es gar nicht so schwer, mit digitaler Selbstverteidigung zu beginnen.

Wer sich im Internet bewegt, muss davon ausgehen, dass die dabei anfallenden bzw. entstehenden Daten fast vollständig von privaten Akteuren und staatlichen Institutionen erfasst werden und für kommerzielle Zwecke oder Überwachung aufbereitet werden. Wie man sich dagegen teilweise schützen kann, wurde kürzlich in einem Beitrag auf Rubikon dargestellt (https://www.rubikon.news/artikel/nichts-bleibt-verborgen).

Schützen kann man sich aber auch in einem weiteren Bereich: Durch Verschlüsselung der Kommunikation mit E-Mails.

Warum Verschlüsselung?

Die E-Mail-Anwendung ist ein sehr frühes Kind des Internets. Bei der Entwicklung war an die Übermittlung sensibler Daten noch nicht gedacht worden, geschweige denn an den heute gängigen Missbrauch mit Spam oder betrügerischen E-Mails. So kam es, dass der Inhalt von E-Mails auf dem Weg vom Absender zum Empfänger ohne Probleme von den Betreibern der Rechner, über die der Weg der E-Mail führt, gelesen werden kann. Vergleichbar ist das mit dem Versand einer Postkarte. E-Mails erreichen in der Regel ihr Ziel nicht auf dem räumlich kürzesten Weg, sondern über mehrere Stationen auf dem schnellsten Weg, auf dem jeweils der Inhalt der E-Mail von den Betreibern dieser Zwischenstationen gelesen werden kann. Seit den Snowden-Enthüllungen ist bekannt, dass dies

auch geschieht und E-Mails systematisch und flächendeckend ausgeforscht werden.

Wie kann man sich dagegen schützen? Beim Postversand würde man sensible Daten in einem Brief versenden, bei E-Mails kann man sich durch Verschlüsselung schützen.

Oftmals wird beklagt, dass man doch keine E-Mail-Partner habe, die ebenfalls Verschlüsselung anwenden, die also verschlüsselte E-Mails empfangen oder versenden können. Das stimmt leider bisher in der Regel. Vorgebracht wird auch, dass man doch nichts zu verbergen habe. Das mag stimmen. Es gibt aber Gruppen von Menschen, die etwas zu verbergen haben: Anwälte, Steuerberater, Mediziner, Menschen in pädagogischen oder sozialen Berufen, Journalisten, usw. Sie müssen darauf vertrauen können, dass ihr E-Mail-Verkehr nicht mitgelesen wird.

Verschlüsselung der E-Mails leistet das. Hilfreich wäre es dabei, wenn mehr Menschen ihre E-Mails verschlüsseln würden, auch wenn der Inhalt belanglos ist. Dann wäre Verschlüsselung unauffällig und die E-Mails der Personen, die Verschlüsselung benötigen, wären nicht so leicht als vielleicht lohnendes Ziel von Angriffen erkennbar.

Es gibt aber eine Anwendung der Verschlüsselung, die auch ohne Partner und Inhalte, die geschützt werden müssen, sinnvoll ist: Die digitale Unterschrift der E-Mail, die Signatur. Sie ist mit einer beglaubigten Unterschrift unter Brief oder Postkarte zu vergleichen.

Wenn man seine E-Mails signiert, kann der Empfänger zweifelsfrei überprüfen, wer der Absender der E-Mail ist und ob die E-Mail auf dem Weg zum Empfänger verändert wurde. Dazu muss der Empfänger aber auf seinem Rechner ein Programm für die Verschlüsselung installiert haben.

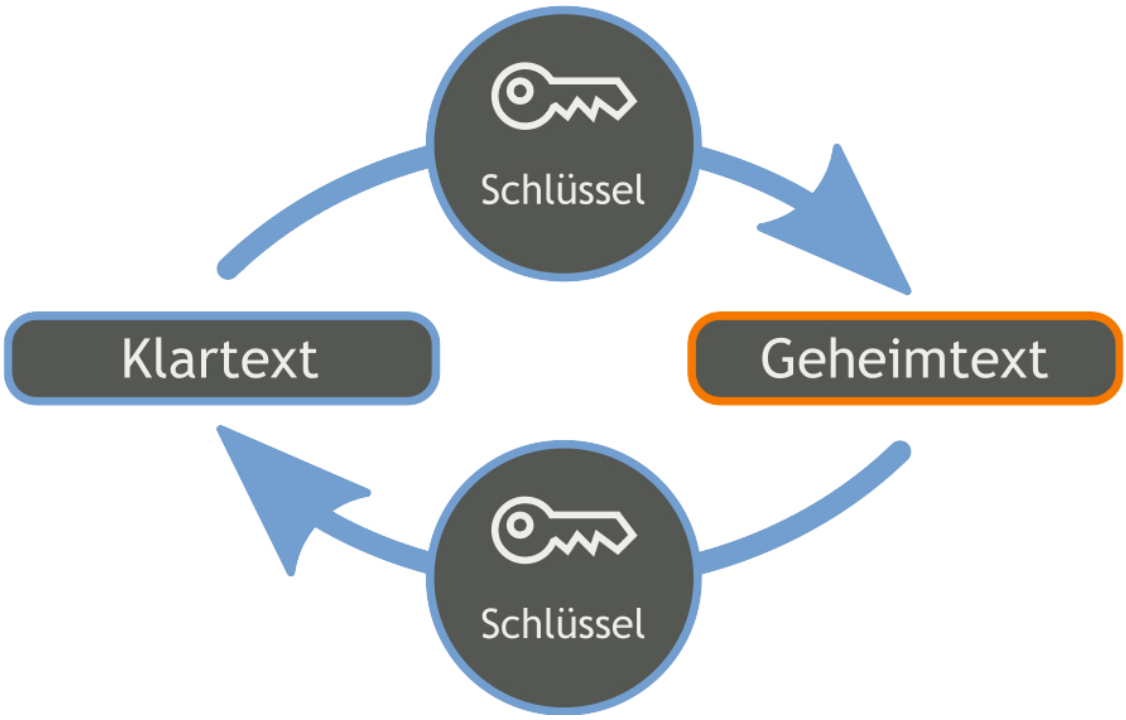
Mit der Verwendung der Signatur fordert man den Empfänger also auf, auch mit der Verschlüsselung zu beginnen. Enthält eine E-Mail Inhalte, bei denen er sicher sein muss, dass sie unverändert sind und wer der Absender ist, wird er wohl mit der Verschlüsselung beginnen.

Auf eine wichtige Einschränkung der E-Mail-Verschlüsselung muss aber hingewiesen werden: Verschlüsselt wird nur der Inhalt der E-Mail! Wie bei einem Brief, bei dem Absender und Empfänger erkennbar sind, sind die sogenannten Metadaten, das sind z.B. Absender, Empfänger, Datum, usw. nicht verschlüsselt. Die können auch bei Anwendung der E-Mail-Verschlüsselung weiterhin ausgeforscht werden. Auch der Betreff der E-Mail wird nicht verschlüsselt und sollte ggf. weggelassen werden.

Wie funktioniert Verschlüsselung?

Bei der Verschlüsselung werden Daten mit einem Schlüssel (eine geeignete Folge von Zeichen) in einem mathematisch sehr aufwändigen Verfahren verschleiert. Vergleichen kann man das damit, dass der Inhalt der E-Mail in einen Tresor gelegt wird, der dann verschlossen und zum Empfänger transportiert wird.

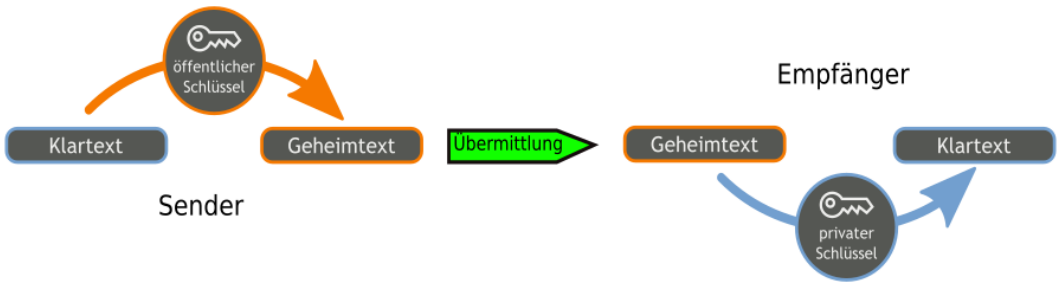
Damit der Empfänger den Tresor aufschließen kann, muss er über einen passenden Schlüssel verfügen. Ist das der gleiche Schlüssel, der für das Abschließen verwendet wurde, kann der Absender den Tresor wieder aufschließen - und jeder, der Zugang zum Schlüssel bekommt!



Wird für die Verschlüsselung und Entschlüsselung der gleiche Schlüssel verwendet, spricht man von **symmetrischer** Verschlüsselung. Bei der symmetrischen Verschlüsselung muss der Schlüssel auf einem sicheren Weg vom Absender zum Empfänger gelangen, dabei könnte er aber entwendet werden. Ein Angreifer könnte auch dem Absender den Schlüssel entwenden, ohne dass dies der Empfänger feststellen könnte. Die symmetrische Verschlüsselung birgt also einige Risiken und wird deshalb für die E-Mail-Verschlüsselung nicht verwendet.

Lösung für dieses Problem ist die **asymmetrische** Verschlüsselung, die man sich folgendermaßen vorstellen kann: Es wird ein Tresor entwickelt, den man mit einem Schlüssel abschließen und **nur** mit einem anderen Schlüssel aufschließen kann. Der Mensch, der verschlüsselte Nachrichten empfangen will, verteilt Tresore und den Schlüssel, mit dem man den Tresor verschließen kann. Dies ist der **öffentliche** Schlüssel. Den Schlüssel für das Öffnen des Tresors, den **geheimen** oder privaten Schlüssel, gibt er nicht weiter und verwahrt ihn sorgfältig an einem geheimen, verschlossenen Ort, für den wiederum nur er den Schlüssel hat. Will ein Absender dem Empfänger eine geheime Nachricht zukommen lassen, legt er sie in den Tresor, verschließt ihn und übermittelt den Tresor dem

Empfänger, der nun den geheimen Schlüssel aus dem Versteck holt, damit den Tresor öffnet und die Nachricht liest.



Zu beachten ist, wie oben schon erwähnt, dass **Absender und Empfänger** des Tresors **bekannt** sind, zudem wird der **Betreff** der Nachricht **nicht verschlüsselt**. Die Kommunikation erfolgt also nicht anonym.

Voraussetzung für die verschlüsselte Kommunikation ist, dass Absender und Empfänger jeweils einen **öffentlichen** und einen **privaten** Schlüssel haben. Mit dem öffentlichen Schlüssel des Empfängers wird die Nachricht vom Absender verschlüsselt, nach der Übermittlung wird sie mit dem privaten Schlüssel des Empfängers **ent**schlüsselt

Die asymmetrische Verschlüsselung ist diejenige, welche für die Verschlüsselung von E-Mails und Dateien verwendet wird. Also:

> ***Verschlüsselt wird vom Absender mit dem öffentlichen Schlüssel des Empfängers, entschlüsselt wird mit dem geheimen Schlüssel des Empfängers.***

Einrichtung der Verschlüsselung

Verschlüsselung gilt als schwer einzurichten. Dies gilt aus meiner Sicht aber nicht mehr, die Einrichtung ist nicht schwieriger als z.B.

die Programmierung eines digitalen Videorekorders.
Mit der von der Free Software Foundation (FSF) herausgegeben **Anleitung zur Einrichtung der E-Mail-Verschlüsselung für alle gängigen Betriebssysteme** (https://emailselfdefense.fsf.org/de/) sollte das gelingen.

Wie der Anleitung zu entnehmen ist, benötigt man für die E-Mail-Verschlüsselung

- ein E-Mail-Programm, das für Verschlüsselung vorbereitet ist: z.B. Thunderbird von der Organisation Mozilla herausgegeben, die auch den Webbrowser Firefox entwickelt);
- ein Programm, mit dem man den geheimen und den öffentlichen Schlüssel erzeugen kann, das die Schlüssel verwaltet und das die eigentliche Ver- und Entschlüsselung erledigt: GnuPG;
- ein Programm, das für die Zusammenarbeit der beiden Programme sorgt. Verwendet wird hier Enigmail, ein Plug-In für Thunderbird. Die Anleitung der FSF beschreibt die Installation und Einrichtung dieser Programme.

Erzeugung und Umgang mit den Schlüsseln

Nach der Einrichtung des eigenen E-Mail-Kontos in Thunderbird müssen als Erstes der private und öffentliche Schlüssel, das Schlüsselpaar, erzeugt werden.Wählen Sie bei der Erzeugung des Schlüsselpaares (der geheime und private Schlüssel in einem Arbeitsgang erzeugt) eine ausreichende Schlüssellänge, damit er nicht zu schnell durch die kontinuierliche Steigerung der Rechenleistung unsicher wird. 4096 Bit Schlüssellänge sollten es gegenwärtig mindestens sein. Die Dauer der Erzeugung hängt von der Länge des Schlüssels ab. Auf alter Hardware kann die Erzeugung also durchaus längere Zeit in Anspruch nehmen. Das erzeugte Schlüsselpaar muss durch ein ausreichend starkes Passwort, die

sogenannte **Passphrase**, geschützt werden. Der geheime Schlüssel und die Passphrase für den Zugang zum geheimen Schlüssel müssen sorgfältig und für andere unzugänglich aufbewahrt werden, z.B. auf einem USB-Stick.

Bei der Erzeugung der Schlüssel sollte ein **Verfallsdatum** eingegeben werden, damit der Schlüssel seine Gültigkeit verliert, wenn er verloren gehen oder unbrauchbar werden sollte. Gleichfalls sollte ein **Widerrufszertifikat** erzeugt werden, mit dem man den Schlüssel für ungültig erklären kann. Mit Enigmail kann all dies leicht erledigt werden.

Der öffentliche Schlüssel sollte möglichst weit verbreitet werden, z.B. indem er auf einen **Schlüsselserver** (Keyserver) hochgeladen wird oder im Fuß der E-Mails verteilt wird. Ein Schlüsselserver ist ein ans Internet angebundener Computer, der die Aufgabe hat, öffentliche Schlüssel zu speichern und im Netz der Schlüsselserver zu verbreiten. Man kann auf Schlüsselservern nach öffentlichen Schlüsseln z.B. für eine E-Mail-Adresse suchen.

Öffentlichen Schlüsseln darf man nicht so ohne Weiteres vertrauen. Ist der Schlüssel gefälscht, können sensible Daten an den falschen Empfänger geraten. Im günstigsten Fall sollte man die Schlüssel persönlich austauschen. Ist das nicht möglich, sollte man den sogenannten **Fingerprint** des Schlüssels auf einem sicheren Weg, z.B. telefonisch, vergleichen. Der Fingerprint ist eine Kette von Zahlen, die bei der Schlüsselerstellung erzeugt wird, mit der man einen öffentlichen Schlüssel eindeutig identifizieren kann.

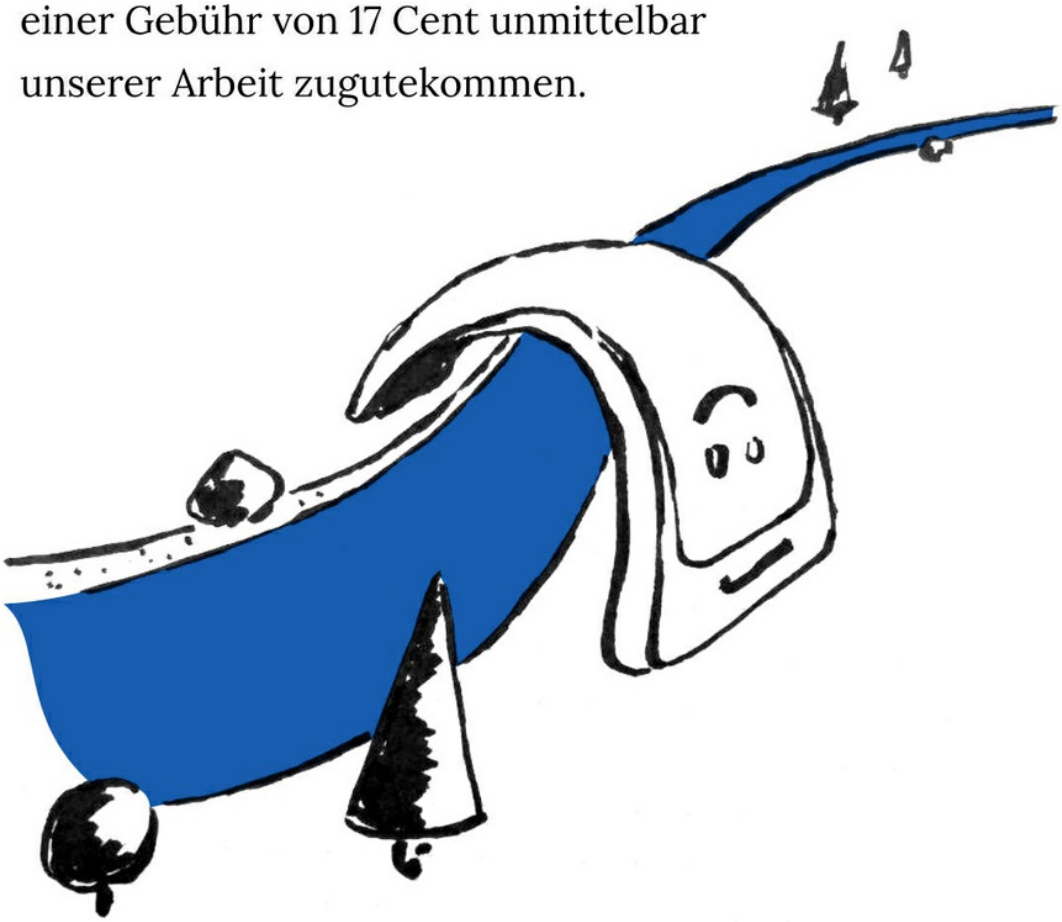
Will man nun eine verschlüsselte oder signierte E-Mail verschicken, wählt man dies im E-Mail-Programm aus. Ggf. muss man noch den öffentlichen Schlüssel des Empfängers auf einem Schlüsselserver suchen und in das E-Mail-Programm importieren. Vor dem Versenden der E-Mail wird man dann nach der eigenen Passphrase gefragt und die E-Mail wird signiert und/oder verschlüsselt

verschickt.

Empfängt man eine E-Mail, die mit dem eigenen öffentlichen Schlüssel verschlüsselt wurde, muss man ebenfalls die Passphrase eingeben, danach wird die E-Mail entschlüsselt und lesbar dargestellt. Die Eingabe der Passphrase ist nach der Einrichtung der einzige zusätzliche Aufwand bei der Verwendung der E-Mail-Verschlüsselung. Sie wird aber in der Regel eine gewisse Zeit im Arbeitsspeicher des Rechners gespeichert, so dass man sie bei der Verwendung des E-Mail-Programms nur einmal eingeben muss, und aus Sicherheitsgründen nach einer einstellbaren Zeit gelöscht.

Hat Ihnen dieser Artikel gefallen?

Dann unterstützen Sie unsere Arbeit auf die denkbar schnellste und einfachste Art: per SMS. Senden Sie einfach eine SMS mit dem Stichwort **Rubikon5** oder **Rubikon10** an die **81190** und mit Ihrer nächsten Handyrechnung werden Ihnen 5,- bzw. 10,- Euro in Rechnung gestellt, die abzüglich einer Gebühr von 17 Cent unmittelbar unserer Arbeit zugutekommen.



Wolfgang Romey arbeitete nach dem Studium der Theoretischen Elektrotechnik als Lehrer für Mathematik, Elektrotechnik und Digitaltechnik im Berufsbildenden Bereich, später als Lehrerausbilder im

Vorbereitungsdienst, dem Referendariat. Dann folgte ein Wechsel in die Bezirksregierung Düsseldorf als Dezernent für Lehrerausbildung und später auch -fortbildung. Er verfügt über etwa 20 Jahre Erfahrung darin, angehende Lehrerinnen und Lehrer auf die Bildungsarbeit mit Digitalen Medien vorzubereiten und deren Urteilskraft in diesem Feld zur Entfaltung zu verhelfen. Die kritische Auseinandersetzung mit den dramatischen Folgen der Digitaltechnik, die ihm extrem unterentwickelt scheint, ist bis heute sein Thema.