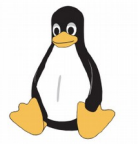
Verschlüsselung von E-Mails und Dateien



Die Anwendung von Verschlüsselung ist doch schwer!

Nein, einmal eingerichtet entsteht fast kein Mehraufwand.

Warum Verschlüsselung?

Wie würden Sie reagieren, wenn Sie Ihre Gehaltsabrechnung, Ihre Bankverbindung, einen Vertragsentwurf, den "blauen Brief" Ihres Kindes, die Rechnung Ihres Psychiaters auf einer Postkarte erhalten würden?

Würden Sie Ihren Freunden Ihre Abwesenheit in den nächsten zwei Wochen auf einer Postkarte mitteilen? Ihre Krankengeschichte? Eine Mahnung?

Selbstverständlich nicht! Das gehört in einen Brief.

Derartige personenbezogene, private, sensible oder vertrauliche Daten werden aber sehr häufig in einer E-Mail übermittelt. Und dann sind sie öffentlich wie auf einer Postkarte.
E-Mails sind 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 für Spams oder betrügerische 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.
E-Mails erreichen in der Regel ihr Ziel nicht auf dem kürzesten Weg, sondern über mehrere Stationen, auf denen jeweils der Inhalt der E-Mail gelesen werden kann, auf dem schnellsten Weg, der länger sein kann als der kürzeste.
Zudem ist ja seit den Snowden-Enthüllungen bekannt, dass E-Mails systematisch und flächendeckend ausgeforscht werden.

Was tun? Verschlüsseln Sie Ihre E-Mails!

Aber ich habe doch keine Partner, die Verschlüsselung anwenden!

Das stimmt leider bisher in der Regel. Es gibt aber eine Anwendung von Verschlüsselung, die auch ohne Partner sinnvoll ist: Die digitale Unterschrift der E-Mail, die Signatur. Sie ist mit einer beglaubigten Unterschrift unter Brief oder Postkarte zu vergleichen.

Wenn Sie Ihre E-Mails signieren, kann der Empfänger überprüfen, dass Sie der Absender der E-Mail sind und Ihre E-Mail nicht 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 fordern Sie den Empfänger also auf, auch mit der Verschlüsselung zu beginnen. Enthält Ihre E-Mail Inhalte, bei denen er sicher sein muss, dass sie unverändert sind, wird er wohl mit der Verschlüsselung beginnen.

Was brauche ich für die Verschlüsselung und das Signieren der E-Mails?

Ein E-Mail-Programm, das mit einem Verschlüsselungs-Programm zusammen arbeiten kann, und ein Programm, das die eigentliche Verschlüsselung erledigt.

Wie funktioniert Verschlüsselung?

Bei der Verschlüsselung werden Daten mit einem Schlüssel in einem mathematisch sehr aufwändigen Verfahren verschleiert. Vergleichen kann man das damit, dass die Daten in einen Tresor gelegt werden, der dann verschlossen und zum Empfänger transportiert wird. Der Empfänger kann den Tresor wieder aufschließen.

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 auch der Absender den Tresor aufschließen. Und jeder, der Zugang zum Schlüssel bekommt! Werden 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.

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 mit dem 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 der 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, dass **Absender und Empfänger** des Tresors **bekannt** sind, zudem wird der **Betreff** der Nachricht **nicht verschlüsselt**. Die Kommunikation erfolgt also nicht anonym, der Betreff ist ggf. wegzulassen. 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 verschlüsselt, entschlüsselt wird sie mit dem privaten Schlüssel des Empfängers.

Die asymmetrische Verschlüsselung ist die, die für die Verschlüsselung von E-Mails und Dateien verwendet wird. Man benötigt dafür

- ein E-Mail-Programm, das für Verschlüsselung vorbereitet ist: dies ist hier das Programm Thunderbird;
- ein Programm, mit dem den geheimen und den öffentlichen Schlüssel erzeugen kann und das die

eigentliche Ver- und Entschlüsselung erledigt: OpenPGP;
- ein Programm, das für die Zusammenarbeit der beiden Programme sorgt. Verwendet wir hier Enigmail.

Erzeugung und Umgang mit den Schlüsseln

Wählen Sie bei der Erzeugung der Schlüssel (der geheime und private werden zusammen erzeugt) eine ausreichende Schlüssellänge, damit er nicht zu schnell durch die technische Entwicklung unsicher wird. 4096 Bit Schlüssellänge (also 4096 Stellen mit den Werten 0 oder 1) sollten es 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.

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.

Der geheime Schlüssel und der Schlüssel für den Zugang zum geheimen Schlüssel, die sogenannte Passphrase, müssen sorgfältig aufbewahrt werden.
Der öffentliche Schlüssel sollte möglichst weit verbreitet werden, z.B. indem er auf einen Schlüsselserver (Keyserver) hochgeladen wird oder im Fuß von 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 Schlüssel z.B. für eine E-Mail Adresse suchen.

Öffentlichen Schlüsseln darf man nicht so ohne Weiteres vertrauen. Im günstigsten Fall sollte man die Schlüssel persönlich austauschen. Ist das nicht möglich, sollte man den sogenannten Fingerprint des Schlüssels auf einem sicheren Weg vergleichen. Der Fingerprint ist eine Kette von Zahlen, mit der man einen öffentlichen Schlüssel eindeutig identifizieren kann.

Einige links:
https://emailselfdefense.fsf.org/de/
Anleitung zur Einrichtung der E-Mail-Verschlüsselung für alle gängigen Betriebssysteme

https://www.privacy-handbuch.de/handbuch_11.htm
Umfassendes Handbuch zu allen Aspekten der Privatheit bei der Nutzung des Internets und digitaler Geräte