Volksverschlüsselung läuft vom Stapel

Massentauglich E-Mails verschlüsseln

Authentifizieren, verschlüsseln, signieren: Was kompliziert klingt, soll mit der Volksverschlüsselung für jedermann handhabbar sein. Der Service ist nun gestartet, derzeit aber nur für Windows-Nutzer verfügbar.

Von Dennis Schirrmacher

Mit der jüngst gestarteten Volksverschlüsselung will das Fraunhofer-Institut für Sichere Informationstechnologie (Fraunhofer SIT) den Ende zu Ende verschlüsselten Versand von E-Mails kostenlos mit wenigen Klicks für jedermann handhabbar machen. Als Partner holten sie sich Ende 2015 die Deutsche Telekom mit ins Boot, die die Infrastruktur stellt.

Hinter der Volksverschlüsselung verbirgt sich ein Unterbau zur Erzeugung, Zertifizierung und Verteilung von Schlüsseln, damit Anwender E-Mails verschlüsselt versenden können. Das gelingt zwar mit PGP schon seit den 90er Jahren, fordert aber viel Einsatz von Nutzern bei der Schlüsselverwaltung. Ein Aufwand, der viele abschreckt. Zudem ist die mobile PGP-Nutzung auf Smartphones und Tablets nicht alltagstauglich.

Für die Verschlüsselung setzt das Fraunhofer SIT nicht auf eine Eigenentwicklung, sondern auf den bewährten S/MIME-Standard und X.509-Zertifikate, die alle E-Mail-Programme bereits unterstützen. So ist die Volksverschlüsselung von Haus aus mit den E-Mail-Clients MS Outlook, Thunderbird und den Webbrowsern Internet Explorer, Chrome und Firefox kompatibel. Eine Nutzung ist auch mit Webmail-Diensten möglich; dafür hält das Fraunhofer SIT derzeit Ausschau nach Partnern. Die Webbrowser tauchen in der Liste auf, da die Volksverschlüsselung in der Theorie auch das Surfen über ein Zertifikats-Handshake vertrauenswürdiger gestalten kann; das kommt in der Praxis aber im Grunde nicht zum Einsatz.

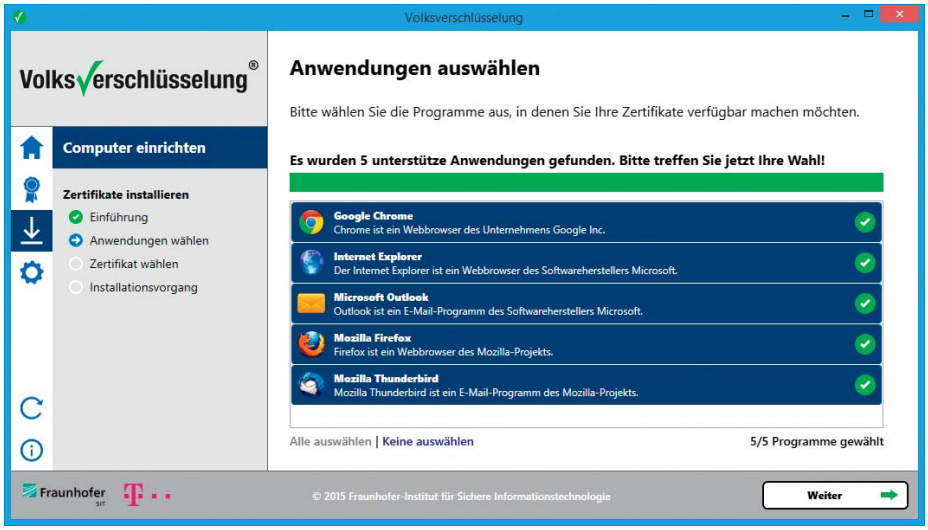
Den Kern bildet die Open-Source-Anwendung Volksverschlüsselung, welche Nutzer bei der Authentifizierung, Erzeugung der Schlüssel und deren Einbettung in das System unterstützt. Derzeit ist die Anwendung ausschließlich für Windows verfügbar. Versionen für Android, iOS, Linux und OS X sollen folgen.

Vorgehensweise

Für einen Schlüssel muss der Anwender seine Identität nachweisen. Aktuell ist dies über die eID-Funktion des elektronischen Personalausweises in Verbindung mit einem Chipkarten-Lesegerät möglich. Telekom-Kunden können die Registrierung mit ihren Log-in-Daten über die Volksverschlüsselungs-Anwendung anstoßen. Alternativ kann man sich auf einer Veranstaltung direkt am Fraunhofer-SIT-Stand für den Service anmelden.

Die kryptografischen Schlüssel erzeugt die Volksverschlüsselungs-Anwendung immer auf dem jeweiligen Endgerät. Der private Schlüssel verbleibt dem Fraunhofer SIT zufolge in den Händen des Nutzers. Die öffentlichen Schlüssel verwaltet wiederum ein Server, der quasi das öffentliche Adressbuch der Volksverschlüsselung darstellt. Bei Bedarf kann man sich aber auch gegen eine Veröffentlichung entscheiden. Die Infrastruktur betreibt die Telekom in einem Hochsicherheitsrechenzentrum. Kommt ein privater Schlüssel abhanden, kann man diesen über die Volksverschlüsselungs-An-

Einstiegshürde: Aktuell kann man sich ausschließlich mit einem elektronischen Personalausweis, den Log-in-Daten eines Telekom-Accounts oder einem zum Beispiel auf Messen erhältlichen Registrierungscode für die Volksverschlüsselung anmelden.



Momentan können ausschließlich Windows-Nutzer von der Volksverschlüsselung profitieren. Android-, iOS, Linux und OS-X-Versionen sind für einen späteren Zeitpunkt geplant.

wendung sperren und einen neuen beantragen.

Mit dem Open-Source-Ansatz gibt sich die Volksverschlüsselungs-Anwendung offen. So können sich Interessierte davon überzeugen, dass sich im Programmcode keine Hintertüren verstecken. Zum Zeitpunkt dieses Artikels war der Code noch nicht verfügbar. Als Vertrauensanker installiert die Anwendung eine eigene Root-CA im System beziehungsweise den Anwendungen. Die anderen im System verankerten CAs werden aber natürlich auch weiterhin genutzt. In Zukunft soll die Volksverschlüsselung auch OpenPGP unterstützen.

Lobenswerter Ansatz

Der Ansatz der Volksverschlüsselung, die Ende zu Ende verschlüsselte Kommunikation via E-Mail massentauglich zu machen, ist zu begrüßen. Denn PGP schreckt viele Nutzer aufgrund seiner sperrigen Usability ab. Doch bereits der unabdingbare Identitätsnachweis über die aktuell drei angebotenen Methoden kann für viele eine unüberwindbare Einstiegshürde sein. Hat man das über die Bühne gebracht, geht die weitere Einrichtung im Gegensatz zu PGP erfreulicherweise simpel vonstatten und man kann nach wenigen Minuten loslegen.

An ein paar Stellschrauben muss das Fraunhofer SIT aber definitiv noch drehen. Vor allem sollten sie zügig die versprochenen Versionen für andere Betriebssysteme und Smartphones nachreichen, um letztlich dem hochgesteckten Ziel der Volksverschlüsselung gerecht zu werden. *(des@ct.de)*

E-Mail-Verschlüsselung

Im August 2013 verkündeten die großen E-Mail-Provider GMX, T-Online und Web.de, dass sie E-Mails untereinander und zum Kunden künftig nur noch über transportverschlüsselte Verbindungen transportieren würden. Bis dahin war es üblich, E-Mails komplett unverschlüsselt durchs Netz zu schicken. Die Verschlüsselung der Mails selbst ist aber immer noch die Ausnahme. Der bislang verbreitetste Standard hierfür ist PGP (Pretty Good Privacy).

Die großen Mail-Provider wie die United-Internet-Marken **GMX** und **Web.de** sowie **T-Online** empfehlen ihren Kunden inzwischen den Einsatz von Mailvelope zur PGP-Verschlüsselung. Mailvelope ist ein Webbrowser-Plug-in, mit dem sich PGP-Mails im Browser ver- und entschlüsseln lassen.

Auf E-Mails spezialisierte Anbieter wie **Posteo** und **Mailbox.org** bieten PGP-Nutzern mehr Funktionen und Komfort. So kann man eingehende Mails sofort beim Empfang mit dem eigenen Schlüssel verschlüsseln.

Der gesetzlich geregelte Dienst **De-Mail** setzte zunächst auf eine Abschottung des Systems nach außen und die Nutzung von Transportverschlüsselung. Erst im April 2015 ließ der Betreiber auch eine Ende-zu-Ende-Verschlüsselung per PGP zu. Wie andere große Mail-Provider legt De-Mail seinen Nutzern den Einsatz des Plug-ins Mailvelope nahe.

(uma@ct.de)