Volksverschlüsselung

Das Angebot des Fraunhofer-Instituts und der Telekom im Check

Die neue Initiative Volksverschlüsselung soll die E-Mail-Kommunikation sicherer machen, Zugriffe auf den Inhalt von E-Mails verhindern und vor Masseüberwachung schützen. Das Programm wurde vom Fraunhofer Institut für Sichere Informationstechnologie (IST) in Zusammenarbeit mit der Deutschen Telekom entwickelt. Herzstück der Volksverschlüsselung ist eine Software, die alle für die E-Mail-Verschlüsselung erforderlichen Krypto-Schlüssel erstellt und vorhandene E-Mail-Programme automatisch auf die Verschlüsselung einrichtet. Damit soll es auch Laien möglich sein, ohne große Vorkenntnisse und Konfigurationsmaßnahmen E-Mails (inhaltlich) verschlüsselt zu versenden. Als Verschlüsselungstechnik kommt nicht PGP (Pretty Good Privacy) oder OpenPGP zur Anwendung, sondern S/MIME.Quelle

Mit der Volksverschlüsselung", so Michael Waidner, Leiter des Fraunhofer-Instituts für Sichere Informationstechnologie (IST), „können Bürgerinnen und Bürger ihre digitale Souveränität verbessern und sich wirkungsvoll vor unerwünschter Massenüberwachung schützen".Quelle

Frage ist, ob das Angebot die darin gesteckten Erwartungen tatsächlich erfüllt und ob dieses auch für Sportvereine und -verbände eine neue Möglichkeit bietet, die E-Mail-Kommunikation sicherer zu machen.

Das Programm zur E-Mail-Verschlüsselung stand erstmals am 29.06.2016 als Download zur Verfügung. Auch wenn die Initiative von ihrem Anspruch, einen Beitrag dazu zu leisten, „dass Sicherheit durch Verschlüsselung für alle so selbstverständlich wird wie das Anlegen des Sicherheitsgurts im Auto"Quelle noch weit entfernt sein dürfte, ist damit ein erster Schritt gemacht, der in den Medien ein breites – allerdings nicht ungeteilt positives Echo gefunden hat. Welches Ziel sich das Fraunhofer Institut und die Telekom für die Zahl der Nutzer gesetzt haben, ist nicht bekannt. Klar dürfte aber allen Beteiligten sein, dass die Zusammenarbeit aller Anbieter nötig sein wird, um die E-Mail-Verschlüsselung in Deutschland als Standard-Kommunikation zu etablieren. Zur CeBIT 2016 hatten die Mitbewerber Web.de und GMX berichtet, dass eine halbe Million Nutzer die Ende-zu-Ende-Verschlüsselung eingerichtet hätten.Quelle

Schon die Installation wird von Kommentatoren als recht kompliziert eingestuft. Sie ist zudem bisher nur auf Windowssystemen durchführbar. Auch ist die Versendung und der Empfang von „rechtssicheren" Dokumenten aktuell noch nicht möglich Quelle. Zudem ist die Verschlüsselungssoftware bisher laut Homepage der Initiative nur mit bestimmten Browsern, wie Internet Explorer, Chrome und Firefox, kompatibel. Weiterentwicklungen zur Nutzung von anderen Browsern, zur Verbesserung der Nutzerfreundlichkeit und für andere Betriebssysteme über Windows hinaus, sind – so die Initiatoren – fest eingeplant, allerdings gibt es dazu weder einen Zeitplan noch, wie die Suche nach weiteren Unterstützern aus Wirtschaft, Forschung und Politik erkennen lässt, eine gesicherte Finanzierung.

Laut einer Umfrage von Bitkom sollen vor der NSA Affäre im Juli 2013 nur 6 % der Befragten ihre E-Mails verschlüsselt haben, in den Folgejahren waren es 14 %, bzw. 15 %. Erstaunlich ist zudem, dass die Mehrheit mit 59% angab, dass der Partner am anderen Ende der Kommunikation keine Verschlüsselungssoftware nutze und man daher auch selbst keine Verschlüsselungs-Software installiert habe. Es ist allerdings anzunehmen, dass die Bereitschaft, eine Verschlüsselungssoftware einzusetzen, gerade vor dem Hintergrund immer neuer Meldungen zu gehackten E-Mailkonten weiter zunehmen dürfte. Hier kann eine nutzerfreundliche, leicht zugängliche und kostenfreie praktikable Verschlüsselungssoftware eine wichtige Rolle übernehmen.

Volksverschlüsselung

Das Angebot des Fraunhofer-Instituts und der Telekom im Check

Die Idee der Verschlüsselungs-Software setzt scheinbar an der richtigen Stelle an, in diesem Punkt ist sich die Netzgemeinde einig. Deutlich wird dies auch durch die Ergebnisse einer Umfrage des Digitalverbandes Bitkom, die (überraschenderweise) zeigt, dass 64 % der Befragten gerne ihre E-Mails und Daten verschlüsseln würde. Als Haupthinderungsgrund für die Installation einer entsprechenden Software wurde angegeben, dass die bisher angebotenen Lösungen zu kompliziert seien.

Wie arbeitet die Volksverschlüsselung und was bietet sie?

Das Programm zur Volksverschlüsselung ermöglicht die Erstellung und Zertifizierung von Schlüsseln, die zudem in die Anwendungsprogramme verteilt werden. Die Software stellt eine Infrastruktur für kryptografische Schlüssel zur Verfügung und umfasst dabei

- eine Zertifizierungsstelle zur Schlüsselbeglaubigung
- einen Verzeichnisdienst zum Abruf der öffentlichen Schlüssel
- einen Sperrdienst für verlorene Schlüssel. Quelle

Die Software sucht also nach erfolgreicher Installation automatisch auf dem Gerät des Nutzers nach Browsern, E-Mail Programmen und sonstigen Anwendungen, welche die Kryptografie nutzen können. Die Schlüssel und Zertifikate sollen laut Berichten automatisch in die Nutzung eingebracht werden. Die Zertifikate entsprechen dem ITU-T-Standard X.509. Dies ist der meist verbreitete Standard und wird dementsprechend auch von den gängigen E-Mail-Clients und Web-Browsern unterstützt. Die Software steht bisher nur für Windows-Nutzer zur Verfügung. Wer die Software für Mac OS X, Linux, iOS oder Android sucht wird nicht fündig. Eine Entwicklung für die genannten Anwendungen neben Windows ist aber fest eingeplant, der genaue Zeitpunkt ist allerdings nicht zu finden.

Wer die Volksverschlüsselung installieren möchte, muss sich über ein Login der Telekom identifizieren lassen. Alternativ dazu ist eine Registrierung über den elektronischen Personalausweis möglich. Als dritte Möglichkeit gibt es die Vor-Ort-Registrierung, die momentan am Fraunhofer-IST oder auf ausgewählten Messen vorgenommen werden kann. Haken hierbei ist allerdings, dass man Zutritt zur Messe haben muss. Bald soll die Registrierung allerdings auch in Telekom-Shops möglich sein. Nach Identitätsprüfung erhält man eine Karte mit einem 12-stelligen Registrierungscode. Wenn die Installation abgeschlossen ist, nimmt das Programm ohne weitere Maßnahmen des Benutzers selbstständig Verbindung zu den gängigen Browsern sowie zu den E-Mail-Programmen Microsoft Outlook und Mozilla Thunderbird auf.

Ein Blick in die Netzgemeinde zeigt ein durchmischtes Bild über die Benutzerfreundlichkeit und das Anwenden der Verschlüsselungssoftware. Das Bundesinnenministerium zeigt sich in seiner Pressemitteilung vom 28.06.2016 begeistert von der neuen Software. Klaus Vitt, Beauftragter der Bundesregierung für IT teilte dazu mit: „Das neue Angebot zur kostenfreien und nutzerorientierten Ende-zu-Ende-Verschlüsselung durch die Deutsche Telekom AG ist ein wichtiger Beitrag für Deutschland als Verschlüsselungsstandort. Ich hoffe, dass dieses Angebot von vielen Kundinnen und Kunden genutzt wird."

Wie auf golem.de zu lesen ist, werden mit der Installation die Programme Mozillas Network Security und Cryptbibliothek Bouncycastle installiert. Zudem wird ein Root-Zertifikat importiert.

Volksverschlüsselung

Das Angebot des Fraunhofer-Instituts und der Telekom im Check

Auch auf der Plattform chip.de wird die neue Verschlüsselungssoftware unter die Lupe genommen. Michael Humpa aus der Software-Redaktion kommt zu ähnlichen Schlüssen wie die restliche Community. Großartiges „Ansinnen,[…] enormes Potential, Praxis […] noch mit großen Hürden".

Liest man die Berichte in der Netz-Community stechen im Wesentlichen drei Punkte heraus:

- fehlende Komptabilität: aktuell kann die Verschlüsselungssoftware nur von Windows-Usern und nur mit ausgewählten Browsern und E-Mail-Clients angewendet werden;
- geringe Benutzerfreundlichkeit - Hürden bei der Einrichtung und Registrierung;
- wenig offengelegter technischer Hintergrund – bislang kein öffentlich zugänglicher Quelltext.

Hinzu kommt, dass noch viele Fragen offen sind. Dazu gehört auch die Frage, ob eingetragene Vereine die Software kostenfrei nutzen dürfen oder ob sie, wie Firmen behandelt werden und damit kostenpflichtig sind.

Dabei sollte laut heise.de die Volksverschlüsselung eine benutzerfreundliche Alternative gegenüber dem umständlich nutzbaren PGP-Verfahren darstellen. Florian Snow, der als Softwareentwickler tätig ist, sieht den häufig genutzten Begriff „Open Source" nur als Marketinginstrument der Telekom und des Fraunhofer-Instituts. Snow formuliert in seinem Gastbeitrag: „Menschen, die wirklich privat kommunizieren möchten, sollten stattdessen besser Freie Software ohne Spionagefunktion zur Verschlüsselung einsetzen, wie beispielsweise das gut etablierte GnuPG."

Erstaunlich ist, dass bisher weder von Landesdatenschutzbeauftragten noch von der Bundesdatenschutzbeauftragten Stellungnahmen zum Projekt vorliegen.

Ob in Deutschland mit der von der Telekom propagierten Volksverschlüsselung ein Schritt Richtung „Verschlüsselungs-Standort Nr. 1" gemacht wurde, ist auf der Basis des aktuellen Entwicklungsstandes eher zu bezweifeln. Zu viele Puzzlesteine sind noch nicht ausgereift, so z.B. das umständliche Anmeldeprozedere, andere sind noch nicht vorhanden, wie z.B. die Anbindung an Apple-Produkte oder die Bedingungen des Zugangs für Firmen, für Sportverbände und -vereine.

Für Sportvereine und –verbände bietet die Volksverschlüsselung daher, jedenfalls solange die o.g. Problemfelder nicht gelöst sind und auch der Status eingetragener Vereine – kostenfreier Privatbereich oder kostenpflichtiger Firmenkunde – ungeklärt ist, aktuell noch keine grundsätzlich verbesserte Möglichkeit zur Etablierung einer sicheren, verschlüsselten E-Mailkommunikation.

Es bleibt somit abzuwarten, in welche Richtung und mit welchem Engagement die Initiatoren und Betreiber der Volksverschlüsselung ihr Produkt weiter entwickeln werden. Das FA-Datenschutzportal wird in jedem Falle an diesem Thema dran bleiben und Sie auf dem Laufenden halten. (L. Reich / M. Roth)

Auszug aus dem monatlichen Info-Brief (Nr. 38, August 2016, S. 16-18) des Online Datenschutzportals der Führungs-Akademie