Sicheres E-Mail-Chaos

Zu E-Mail gibt es eigentlich nichts mehr zu sagen. Ein jahrzehntealter Dienst mit ausgereiften Protokollen und Programmen. Das dachte wohl auch Mozilla-Chefin Mitchell Baker, als sie ihre Überlegungen zur Thunderbird-Zukunft kundtat. Das Programm müsse weg vom Browser Firefox, der benötige dringend mehr Aufmerksamkeit. Die einst so beliebte Applikation leidet zunehmend unter Nutzerschwund. Eigentlich keine neue Idee, bereits 2007 hatte Baker die Gründung einer separaten Thunderbird-Foundation angeregt.

Und schon seit 2012 gibt es neue Funktionen nur noch von der Community – denn das Programm sei ja fertig entwickelt. Doch das ist bei näherem Hinsehen keineswegs so. Von Haus aus kommt Thunderbird ohne ein Verschlüsselungsmodul, die Nachrichten werden im Klartext verschickt wie Feldpostkarten.

Besonders laut haben darum gegen Bakers Pläne Projekte wie Pretty Easy Privacy (PEP) protestiert. Die PEP-Macher haben sich zum Ziel gesetzt, die Nutzung von PGP nicht nur benutzerfreundlicher zu machen, sondern auch Verschlüsselung per Default mit auszuliefern.

Man muss nur Thunderbird mit integriertem PEP installieren und darauf hoffen, dass die andere Seite irgendwo mal etwas zum Verschlüsseln hinterlassen hat. Hat der Empfänger das nicht, muss er bloß die Umgebung herunterladen und sie installieren. Per Telefonat kann man die Verschlüsselung abschließen. Erinnert so gesehen doch ein bisschen an aktuelle PGP-Implementierungen.

Und dazu bräuchte die Krypto-Gemeinde unbedingt Thunderbird. Eine steile These. Bisher gibt es von PEP bloß eine Preview – für Microsoft Outlook, immerhin der in Unternehmen am weitesten verbreitete Client. Für den Vertrieb von Outlook mit integriertem PEP wird auch schon erfahrenes Personal gesucht.

Und für Thunderbird ist allen Ernstes ein Fork angedacht. Als ob es davon nicht schon genug gäbe. Einfacher machen es einem da ohnehin andere Projekte. Wer eine umfangreiche Alternative zu Outlook will, greift zu Evolution. Spartanisch und effizient geht es mit Mutt auf der Kommandozeile zu. Und Claws Mail bietet einen rationellen Mittelweg: Wer die Gpg4win zur PGP-Verschlüsselung unter Windows installiert, bekommt den Client gleich mitgeliefert. Und alle kommen ohne zusätzliche Plug-ins aus.

Sicher, Pretty Good Privacy ist als kompliziert verschrien, Schlüssel auf Keyservern austauschen und so weiter. Das bekommt doch kein Nutzer hin. Außerdem ist es nicht sehr verbreitet.

Klar: Jede Idee, sichere Kommunikation zu verbreiten, ist willkommen. Aber weder ist Thunderbird das heilige und einzige Juwel der E-Mail-Clients, noch ist PEP momentan schon ein Leuchtfeuer in Sachen Benutzerfreundlichkeit. Statt mit einem Fork-Tohuwabohu die Nutzer zu verwirren, sollte man sich lieber daran machen, vorhandene und funktionierende Ansätze besser zu integrieren.

Doch am Ende hilft das alles nichts, wenn es nicht vor der Tastatur ankommt. Die meisten Nutzer klicken sich lieber per Google-Webmail durch ihre Nachrichten. Ohne den ungeliebten Anwender wird es eben nichts. Wenn der aber nicht einmal bereit ist, das simple Konzept hinter PGP zu lernen, darf man seine Begeisterung für sichere IT grundlegend bezweifeln.

MORITZ FÖRSTER