Wehrt euch!

Verschlüsselt eure E-Mails!

Rechnen wir im Zeitalter nach Snowden, so befinden wir uns im Jahr eins n. S. Nach dem Schock des Erwachens muss langsam damit begonnen werden, nachhaltig zu handeln. Es gibt Wege, E-Mails sicher zu verschlüsseln. Man muss es nur tun!

Text: **Klaus-Peter Löhr**

Seit dem ersten Snowden-Schock ist ein Jahr vergangen. Seitdem haben uns immer neue Enthüllungen in Atem gehalten. Die Empörung war groß, und die langfristigen Folgen sind noch nicht abzusehen. Der Bürger sieht seine Privatsphäre durch unkontrollierbare Ausspähung bedroht und hat das Gefühl, dass die Politik ihn im Stich lässt.

Den meisten Menschen ist allerdings nicht bewusst, dass sie sich an einer Stelle durchaus gegen die Bedrohung wehren können: Jeder ist in der Lage, den Inhalt von E-Mails durch Verschlüsselung zuverlässig auch gegen potente Angreifer zu schützen. Würden alle Bürger ihre E-Mails gewohnheitsmäßig verschlüsseln, wäre das Briefgeheimnis im Netz nicht nur theoretisch garantiert, sondern auch technisch gesichert.

Warum geschieht das nicht?

Weil wir beim heutigen Stand der Technik nicht erwarten können, dass Erika Mustermann sich der Mühsal der E-Mail-Verschlüsselung unterzieht. Von wenigen Ausnahmen abgesehen ist die einschlägige Software nicht benutzerfreundlich.

Als Informatiker haben wir daher die wichtige Aufgabe, in Forschung und Entwicklung das bisher Versäumte nachzuholen. Als Staatsbürger sollten wir aber nicht einfach auf den großen technischen Wurf warten, sondern fragen, wie wir uns der konkreten Utopie einer flächendeckenden E-Mail-Verschlüsselung bereits heute annähern können: Es gilt, die vorhandenen Möglichkeiten konsequent zu nutzen und evolutionär zu verbessern.

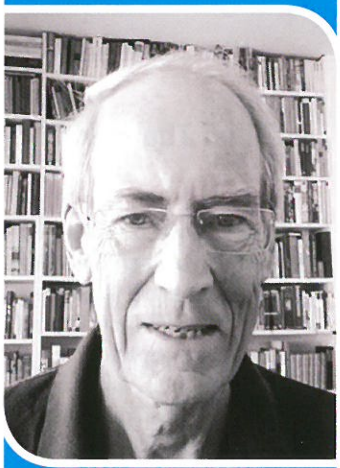
Zwei Verfahren

Wer heute E-Mails verschlüsseln will, hat die Wahl zwischen S/MIME und PGP. Beide bieten die gleiche kryptographische Sicherheit. Hier ist nicht der Ort, das Pro und Contra der beiden Ansätze im Detail zu diskutieren. Meine eigene Position ist: Im Hinblick auf das Ziel der flächendeckenden Verschlüsselung für jedermann ist S/MIME die bessere Wahl: Der S/MIME-Standard wird von jedem Mail-Programm unterstützt, und mit einer gut gestalteten Web-Schnittstelle sind Schlüsselerzeugung und Zertifikatserwerb kinderleicht. (Die Verwaltung und Benutzung des Schlüsselbunds gestaltet sich allerdings je nach Hersteller unterschiedlich – von trivial bis umständlich.)

Ein Plädoyer für S/MIME ist aber letztlich nur dann vertretbar, wenn es gelingt, Zertifizierungsstellen zu schaffen, die erstens einfach, zweitens kostenlos und drittens vertrauenswürdig sind; kritisch ist weniger Punkt 2 als vielmehr Punkt 3: Es bedarf einer offenen Zertifizierungsstelle, der aufgrund ihrer Konstruktion jeder Bürger vertrauen kann (wie man dem Wahllokal vertraut). Dies wäre eine noble Aufgabe beispielsweise für eine staatsbürgerlich engagierte Stiftung.

Um aber schließlich auf die Verantwortung der Politik zurückzukommen: Hier zeigt sich eine Möglichkeit, wie etwas von dem Vertrauen, das die Regierung durch ihr Verhalten in der Snowden-Affäre verloren hat, wiedergewonnen werden könnte. Der Innenminister könnte die Gründung einer Zertifizierungsstiftung betreiben und damit zeigen, dass er konkret etwas zum Schutz unserer Privatsphäre tut. Wehren müssen wir uns schon selbst, aber die Politik sollte uns wenigstens nach Kräften dabei unterstützen. ●

autor



Prof. (a. D.) Dr.-Ing. Klaus-Peter Löhr, Fachbereich Mathematik und Informatik, Freie Universität Berlin; Fellow der Gesellschaft für Informatik; Mitglied des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung.

Bildquelle: privat