Interview

«Verschlüsselung sollte Standard sein»

Alle wollen sie an unsere kostbaren Daten: Geheimdienste, Suchmaschinen, Mailprovider und Supermärkte. Die langfristigen Konsequenzen dieses globalen Data-Mining sind dabei nur schwer abzuschätzen. Doch es gibt Alternativen. Das Projekt immerda.ch ermöglicht seit 15 Jahren seinen Nutzenden eine sichere und private Kommunikation. Das Megafon hat sich mit dem Administrator Paul zum Gespräch getroffen. Teil 1 von 2.

Interview: res | Illustration: pak

megafon: *Worin unterschiedet sich eurer Mailprogramm von anderen Providern?*

Paul: Der Hauptunterschiede liegt darin, dass wir uns nicht über Werbung finanzieren sondern über Spenden. Wir arbeiten alle freiwillig und in unserer Freizeit. Wir haben deshalb auch kein Interesse daran, unsere Nutzerinnen auszuspionieren und mit ihren Daten Geld zu verdienen.

Ist das Ausspähen und Datenauswerten der User sozusagen das Standard-Geschäftsmodell der normalen, vermeintlich kostenlosen Mail-Providern?

Ja, aber das gilt ja im Prinzip für fast alle Gratis-Angebote im Internet. Es ist eben nicht gratis, sondern du finanzierst es auf eine Weise, die dir auf den ersten Blick nicht auffällt. Einerseits konsumierst du Werbung, andererseits generierst du Daten, welche die entsprechende Firma weiterverkaufen kann. Dadurch wird das entsprechende Produkt finanziert.

Gmail sammelt so viele Daten seiner User wie möglich. Andererseits ist der Dienst gegen Angriffe von Aussen heute recht sicher...

Es gibt da unterschiedliche Ebenen. Das eine ist, wie viel dein Provider aufzeichnet, also sogenannte Meta-Daten: Wann loggst du dich ein? Mit wem mailst du? Wo befindest du dich? Bei Immerda haben wir hier dazu eine ganz klare Politik: Wir zeichnen grundsätzlich nur auf, was für den Betrieb notwendig ist. Das heisst, wir speichern etwa deine deine IP-Adresse nicht ab. Unter anderem seit Snowden wissen wir, dass viele mit Geheimdiensten kooperieren. Das andere ist die allgemeine Sicherheit. Da ist da recht viel passiert, gerade auch bei den grossen Anbietern. Das ist meiner Meinung nach nicht der Hauptgrund, warum man auf diesen Dienste verzichten sollte.

Es gibt auf immerda die Möglichkeit, seine Mails zu verschlüsseln. Mir ist das leider zu kompliziert. Meine Frage an dich: Verschlüsselst du deine Mails?

Wenn ich kann dann mache ich das. Es kommt natürlich auch auf den Empfänger an, der brauch ja meinen öffentlichen Schlüssel.

> *«Auch ist es relativ einfach Nachrichten zu manipulieren oder zu fälschen.»*

Warum sollte ich meine Mails überhaupt verschlüsseln? Ich bin doch nicht interessant für die Geheimdienste.

Es geht auch darum, dass die Zwischenstationen nicht mitlesen können. Das Problem ist nicht, dass Ueli dein Mail lesen könnte, sondern, dass alle Mails von allen Personen für immer abgespeichert werden können. Das ist ein gesellschaftliches Problem. Auch ist es relativ einfach Nachrichten zu manipulieren oder zu fälschen. End-to-End Verschlüsselung sollte der Standard sein, nicht umgekehrt. Du willst, dass die Nachricht dein Gerät verschlüsselt verlässt und erst vom Empfänger selbst entschlüsselt wird.

Sozusagen der Goldstandard.

Genau, alles andere macht eigentlich keinen Sinn und ist immer nur Flickwerk. Immerda kann zum Beispiel zu einem gewissen Grad die Metadaten schützen. Aber wenn du wirklich sicher sein willst, dass niemand deine Nachricht liest oder verändert, dann führt an der End-to-end Verschlüsselung kein Weg vorbei.

Auf immerda.ch ist das Verschlüsseln der Mails in acht Schritten beschrieben. Das ist doch vielen User viel zu kompliziert...

Du kannst auf dem Webmail ein Schlüssel erstellen, das braucht nur zwei Schritte. Aber ich gebe es zu, es ist nicht ganz einfach, es gibt eine gewisse technische Hürde. Es ist auch nicht ein einfach zu lösendes Problem, auch mathematisch. Wie findet man den Schlüssel des Empfängers? Das ist auch nach 20 Jahren noch ein ungelöstes Problem. Das Internet wurde in einer Zeit entworfen, wo niemand mit einer systematischen Überwachung gerechnet hat.

Wie sieht das bei neuen Diensten aus, etwa für das Smartphone?

Dort sieht es etwas besser aus. Signal funktioniert beispielsweise recht gut. Im Gegensatz zum Mail hat man dort halt einen zentralen Server der die Schlüssel speichert.

Ist Signal also absolut sicher?

Absolut sicher gibt es sowieso nicht. So gibt es bis heute keinen mathematisch sauberen Beweis, dass die Verschlüsselung, die deine Bank braucht, um dein E-Banking abzusichern, nicht zu knacken ist. Was man macht ist sogenanntes Threat-Modelling: Wer ist der Angreifer, was hat er für ein Budget. Zum Beispiel: Kann er nur deinen Anschluss überwachen, kann er alle Anschlüsse überwachen? Dann machst du eine entsprechende Lösung. Aber wenn dann noch etwas dazukommt, zum Beispiel ein Trojaner auf deinem PC, dann ist dein Modell dahin. ■

Der zweite Teil des Interviews folgt im Januar-Heft.

immerda.ch

Immerda wurde 2001 im Umfeld der Anti-WEF- Proteste gegründet. Das Ziel von immerda ist es, Freundinnen und Freunden einfache und sichere Kommunikation zu ermöglichen und ihre Privatsphäre so gut wie möglich zu schützen. Das Projekt finanziert sich ausschliesslich durch Spenden, alle Mitarbeiter arbeiten gratis. Um eine immerda Mailadresse zu bekommen benötigt man eine Einladung.

Spenden:
PC-60-217095-9 | IBAN: CH78 0900 0000 6021 7095 9