2013/29 Disko

https://shop.jungle.world/artikel/2013/29/viel-aufwand-wenig-nutzen

Geheimdienste interessieren sich nicht für Inhalte

Viel Aufwand, wenig Nutzen

Von **Boris Mayer**

Natürlich ist die Verschlüsselung des eigenen Datenverkehrs eine gute Idee, um - Geheimdiensten und anderen Neugierigen das Mitlesen unmöglich zu machen. Doch in der Praxis ist dieses von IT-Profis vielbeschworene Rezept in der heutigen Internetwelt kaum einsetzbar.

Bei einem E-Mail-Programm auf dem PC und bei manch einem auf dem Smartphone lässt sich PGP inzwischen relativ einfach einrichten, und auch ein Schlüsselpaar aus public und private key ist schnell generiert – wenn man weiß, was man zu tun hat. Nach wie vor legen die Entwickler von Crypto-Programmen allerdings nicht viel Wert auf einfache Benutzerführung. Wie bei jedem anderen Tool gilt auch für Security-Programme, dass etwas, das nicht intuitiv und ohne Hilfe anderer bedienbar ist, auch nicht gern verwendet wird (die derzeit vielerorts veranstalteten Crypto-Partys zeigen, wie viel Hilfe Durchschnitt-PC-User bei der Installation der Software brauchen). Dummerweise muss jedoch, damit es mit der verschlüsselten Kommunikation klappt, jeder Kommunikationspartner überzeugt werden, das auch zu tun. Ziemlich viel Aufwand – und dabei sind dann trotzdem nur E-Mails gesichert. Und auch nur die von einem echten Programm auf einem eigenen Gerät verschickten E-Mails. Wer aus Bequemlichkeit lieber einen Webmailer statt Outlook, Apple Mail, Thunderbird verwendet, wird bestimmt nicht Texte aus dem Mailfenster kopieren und mit einem besonderen Programm entschlüsseln wollen, denn das bedeutet noch mehr Aufwand als ein fest installiertes Mailprogramm. Damit fallen alle Webmailnutzer im Freundeskreis bei der Verschlüsselung weg – Encryption funktioniert natürlich nur dann, wenn alle Beteiligten sie nutzen.

Außerdem ist Kommunikation längst nicht mehr nur auf den Austausch von E-Mails beschränkt. Ob man bei Facebook und anderen »social media«-Plattformen chattet oder über Twitter private Nachrichten austauscht, verschlüsselt werden diese Botschaften grundsätzlich nicht übertragen. Es gibt zwar auch Chat-Programme, die encrypted messages übertragen können, aber dann muss man nicht nur alle Bekannten und Kollegen dazu bringen, Verschlüsselung einzusetzen, sondern auch noch dazu, einen ganz anderen Chat zu benutzen – und das ist nicht besonders komfortabel, bekommt man doch erfahrungsgemäß nicht einmal den gesamten Freundeskreis dazu, geschlossen auf ein Crypto-Produkt zu wechseln. Wer schon mal mit zwei oder drei unterschiedlichen Chat-Programmen gleichzeitig online war, weiß, wie viel komplizierter und unübersichtlicher alles dadurch wird; eine einfache Nachricht zu verschicken, dauert dann gleich

doppelt oder dreimal so lange, weil man erst überlegen muss, in welchem Programm wer doch gleich noch zu finden war.
Allein, dass gerade nach dem Aufdecken von Prism, Tempora und Co. alle erst einmal panisch nach einer Lösung rufen, zeigt, dass sich die meisten gar nicht wirklich dafür interessieren – inklusive Politiker. Denn dass der meiste Datenverkehr über das Internet unverschlüsselt abläuft und dass die Geheimdienste an allen möglichen Stellen mitlesen, ist schon seit Ewigkeiten bekannt. Bereits 2001 gab es den Echelon-Skandal, bei dem bekannt wurde, dass der gesamte über Satelliten übertragene Datenverkehr von US-Geheimdiensten abgehört wurde. Damals wurden die IT-Richtlinien von Firmen schleunigst überarbeitet, das Versenden unverschlüsselter E-Mails an Empfänger außerhalb des Hausnetzes wurde verboten. Doch darf man dann zwölf Jahre später eigentlich überrascht sein, dass die Überwachung in dem Jahrzehnt danach ausgeweitet wurde? Eigentlich nicht. Und außerdem nutzt selbst die Bundeskanzlerin ihr Crypto-Phone nur, wenn sie im Ausland ist. SMS schreibt sie in Klartext und unverschlüsselt, genau wie alle anderen auch. So weit kann es mit dem Bedarf nach verschlüsselten Datenverkehr also nicht her sein.

Doch selbst wenn alle plötzlich für alles Verschlüsselung nutzen würden – und das auch funktionierte –, eines würde das nicht verhindern. Viel wichtiger als der Inhalt sind den Geheimdiensten die Verbindungsdaten – auch nach Angaben von Edward Snowden. Der Grund dafür ist klar: Verbindungsdaten sind mit der Hilfe von Computern sehr einfach auszuwerten. Wer kommuniziert wie oft und wie viel auf welchem Weg mit wem? Das ist die Frage, die Geheimdienste wirklich interessiert, denn sie ist nicht abhängig vom Verständnis irgendwelcher unterschiedlicher Sprachen oder Codes. Kommunikation ohne oder nur mit verschlüsseltem Adressaten kommt dagegen nicht an, und wer etwas verschickt, lässt sich auch nur bedingt verschleiern, wenn der Empfänger wissen soll, von wem die Nachricht kommt.
Aus diesen Gründen bringt Verschlüsselung zwar Aufwand mit sich, den gläsernen Bürger macht sie aber nicht viel weniger durchsichtig, um genau zu sein, reicht es nicht mal für einen Milchglas-Bürger. Und deshalb wird sich auch nichts ändern, wenn sich die Aufregung erst einmal ein wenig gelegt hat. Beim nächsten Skandal werden wieder alle überrascht sein, dass die Geheimdienste ihre Techniken verfeinert haben – und alle werden immer noch bei Facebook, Twitter und Co. fröhlich unverschlüsselt Nachrichten austauschen.