Cryptoparty

Vor nur 25 Jahren war es in der DDR normal, dass der Staat Briefe seiner Bürger öffnete und kontrollierte, bevor sie den Empfängern zugestellt wurden. Wer unerwünschte Meinungen vertrat, wurde verfolgt. Im Fichenskandal wurde aufgedeckt, dass auch Schweizer Geheimdienste massenhaft Menschen überwachten und potentielle Arbeitgeber wurden vor der Einstellung «Subversiver» gemahnt. Damals wie heute lösen solche Massnahmen zu Recht Empörung aus.

Mittlerweile wissen wir, dass heute die elektronische Post von uns allen systematisch untersucht und kontrolliert wird. Mit einer zweifelhaften rechtlichen Grundlage wird genau der Kommunikationskanal überwacht, der zunehmend die gute alte Post ablöst. Dass das Post- und Fernmeldegeheimnis eigentlich auch hier gelten sollte, stört die Geheimdienste herzlich wenig. Zur Not werden Eingriffe in unsere Grundrechte mit der angeblich allgegenwärtigen Gefahr des Terrorismus gerechtfertigt. Für private Unterhaltungen bleiben uns also nur wenige Alternativen. Wir könnten wieder Briefe schreiben oder in den Wald gehen und uns auf einer einsamen Lichtung treffen. Oder aber wir beginnen unsere Emails mittels GnuPG zu verschlüsseln, sodass nur der Empfänger ihren Inhalt lesen kann und nicht die gierigen Augen und Ohren des grossen Bruders. Wir können verschlüsselte Chatsysteme wie «Jabber» in Kombination mit Off-the-Record Message (OTR) nutzen, die für den kurzen Austausch weit praktischer als Email sind, da so noch weniger Metadaten anfallen. Und wenn wir gerade dabei sind, können wir auch gleich anonym mittels TOR im Internet surfen und nebenbei freie Software verwenden.

Dock18: Neben vielen anderen OrganisatorInnen tritt auch der Chaos Computer Club als Initiator von Cryptoparties auf. Was sind Cryptoparties?

An der Cryptoparty können alle lernen, wie moderne, starke Verschlüsselungsverfahren verwendet werden können. Es ist nicht teuer, es ist nicht schwierig, es dauert nicht lange – es ist kinderleicht. Die Ansicht, dass so etwas nur Nerds und Hacker können, gehört in die Vergangenheit. Cryptoparties haben sich als weltweite Idee zur Verbreitung von technischem und sozialem Wissen über Kryptographie etabliert. Unter www.cryptoparty.in finden sich die nächsten Parties an verschieden Orten – mit einer Anleitung zum selber Stemmen einer Cryptoparty. Es steht jedem frei selbst solche Veranstaltungen zu organisieren. Bei aller Paranoia soll eine Cryptoparty auch Spass machen. Es geht um das gemeinsame Verstehen von Technik und deren Möglichkeiten unsere Freiheits- und Bürgerrechte zu bewahren. Es geht vor allem um den privaten Schutzraum, der es erst ermöglicht eine individuelle Persönlichkeit zu leben. Ständige Überwachung führt zu gebrochenen Menschen.

Dock18: Vor ca. vier Monaten wurden die ersten Dokumente zur Überwachung des Internets durch amerikanische und andere Geheimdienste veröffentlicht. Seither ist anzunehmen, dass grosse Teile unserer Kommunikation überwacht werden. Was ist eure wichtigste Erkenntnis aus den ganzen Veröffentlichungen? Was hat euch am meisten überrascht?

Die Namen der Programme. Die Inhalte sind wenig überraschend: Viele haben schon lange vor den Veröffentlichungen von Edward Snowden davor gewarnt, dass Geheimdienste und andere staatliche Stellen weltweit massiv Telekommunikation überwawchen. Nun gibt es dafür die Bestätigung eines Insiders. Wer sich die Gesetze ansieht, dem konnte aber schon viel früher klar sein, was alles gemacht werden darf. Für die Existenz dieser Gesetze gibt es einen Grund: Demokratische Staaten dürfen nur machen, was ihnen gesetzlich erlaubt ist. Kein Staat würde sich Überwachung erlauben, wenn er diese nicht einsetzen will.

Dock18: Der Whistleblower Edward Snowden sagte in einem Interview: «Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on.» Wie wir heute wissen, hat er diese Worte sehr präzise gewählt. Der amerikanische Geheimdienst hat es scheinbar geschafft, dass gewisse Verschlüsslungsprotokolle absichtlich einfach knackbar sind. Wie können wir sichergehen, dass wir sicher verschlüsseln?

Grundsätzlich: Freie quelloffene Software nutzen. So sind Backdoors viel schwerer zu verstecken. Auch wenn man natürlich nicht den ganzen Quelltext aller Software, die auf einen Computer läuft, lesen kann: Die Möglichkeit der Entdeckung ist viel höher. Auch reicht es nicht, Thunderbird mit GPG auf Windows zu nutzen, da Windows mit Thunderbird machen kann, was es will.

Dock18: Im Nachgang zur Affäre hat der amerikanische Geheimdienst einen Dienst namens Lavabit, der verschlüsselte und sichere Kommunikation ermöglicht, zur Aufgabe gezwungen. Es wird vermutet, dass Lavabit gezwungen wurde, seine Nutzer heimlich zu überwachen. Das ist dank amerikanischen Sicherheitsgesetzen möglich. Gibt es ein vergleichbares Risiko in der Schweiz?

In der Schweiz existiert kein unmittelbares Risiko, dass der Staat einen Kommunikationsdienstleister zur Aufgabe zwingt. Die Schweiz würde als Wirtschafts- und Technologiestandort unter einer solchen Aktion stark leiden. Die aktuellen Gesetze erlauben es den Schweizer Geheimdiensten nicht, sich im Inland einen Generalzugang zu Daten eines Anbieters zu verschaffen. Allerdings könnte sich dieser Zustand durch das momentan diskutierte neue Nachrichtendienstgesetz ändern. Dieses spricht dem NDB massiv höhere Kompetenzen zu. Wenn dieser dann für sich beansprucht, auf alle Daten von Mailanbietern gleichermassen Direktzugriff zu haben wie die NSA auf die US-Anbieter, könnte dies ähnliche Projekte wie Lavabit in der Schweiz ebenfalls gefährden, weil die Betreiber für die Sicherheit nicht mehr garantieren können.

Dock18: Welches Ausmass hat die Überwachung in der Schweiz angenommen?

Was das Internet angeht, darf man sich keine Illusionen machen: Sehr viele Services sind international gehostet, und ob die Überwachung der Schweizer Dienste weniger weit geht, macht keinen Unterschied. Ausserdem sind im Moment einige Gesetzesänderungen auf dem Weg, die auch die Überwachung digitaler Kommunikation bringen, die noch eher Ländergrenzen kennt: der von Telefon und Handys. Mit den bestehenden Gesetzen dürfen diese überwacht werden, wenn es im Einzelfall richterlich angeordnet ist. Nicht erlaubt ist verdachtsunabhängige Überwachung, ausser der Vorratsdatenspeicherung.

Schülerin (14): «Wie können die meine E-Mails lesen?»

Wenn du ein Mail verschickst, wird dieses an deinen Mailanbieter (z.B. GMX, Bluewin, usw.) übertragen. Dies geschieht jedoch nicht direkt, sondern über ein paar Zwischenschritte, weil es ja keine direkte Leitung zwischen deinem Computer und GMX gibt. Die Zwischenschritte sind Computer, deren Aufgabe eigentlich nur die Weiterleitung deines Mails ist. Allerdings kann jemand, der einen solchen Computer kontrolliert, diesen so programmieren, dass er eine Kopie von jedem Mail an ihn schickt (z.B. an die NSA). Dagegen hilft eine verschlüsselte Verbindung zum Mailanbieter. Nur leider ist die Reise deines E-Mails da noch nicht fertig. Als nächstes muss das Mail zum Mailanbieter des Empfängers geleitet werden. Für diese Verbindung sind dein Mailanbieter sowie der Anbieter des Empfängers verantwortlich; du kannst nicht kontrollieren, ob diese Verbindung ebenfalls verschlüsselt ist. Zum Schluss ruft der Empfänger das Mail noch von seinem Anbieter ab, auch auf diesem Weg kann das Mail gelesen werden.

Es geht aber noch weiter: Auch wenn alle drei Transportwege verschlüsselt werden, können Geheimdienste den Mailanbieter dazu zwingen, eine Kopie von allen Mails, die über den Computer vom Mailanbieter laufen, der NSA zu geben. Die einzige Möglichkeit, ein Mitlesen zu verhindern, ist eine Ende-zu-Ende-Verschlüsselung zwischen dir und dem Empfänger. Dies ist nicht ganz einfach, denn sowohl du als auch der Empfänger müssen eine zusätzliche Verschlüsselungssoftware installieren und einrichten.

Dock18: Vielerorts wird gefordert, dass die Leute sich selber besser schützen und die Kommunikation verschlüsseln. Ist der Fokus auf Selbstverteidigung durch Verschlüsselung nicht auch problematisch? Müsste man nicht grundsätzlich von der Politik in einer Demokratie einfordern, dass sie die Aktivitäten der Geheimdienste und Verletzung der Privatsphäre einschränkt?

Ja, natürlich. Es gibt da aber ein paar Probleme: Es gibt keine weltweite Demokratie, es gibt keine weltweiten Freiheitsrechte. Das Internet ist aber weltweit, wobei viele Entscheidungen und Services in den USA liegen. Und die werfen bekanntermassen alle persönlichen Rechte über Bord, wenn jemand National Security schreit. Ausserdem anerkennt die USA Rechte nur, wenn sie US-Amerikaner betreffen; ein Internet-User ist im Zweifelsfall Ausländer und damit praktisch rechtslos.

Text und Antworten auf Fragen wurden kollektiv von Mitgliedern des Chaos Computer Club Zürich verfasst.

Der Chaos Computer Club Zürich trifft sich jeden Mittwoch 19 Uhr an der Luegislandstrasse 485 in Zürich-Schwamendingen. Die Treffen sind öffentlich.

www.ccczh.ch

Thematischer Veranstaltungshinweis:
8. Cryptoparty, 8. November 2013, 20 Uhr, Dock18

Die Medienkulturgespräche sind eine Reihe des Dock18 Institut für Medienkulturen der Welt.
www.dock18.ch/medienkultur