Warum Verschlüsselung uns sicher und auch frei macht

gelesen: https://www.freitag.de/autoren/the-guardian/auf-beiden-augen-blind?utm_source=pocket-newtab

Auf beiden Augen blind

Überwachung Weltweit führen Regierungen einen Feldzug gegen sichere Kommunikation. Hier erklärt Edward Snowden, warum Verschlüsselung uns nicht nur sicher, sondern auch frei macht

Edward Snowden 7

Edward Snowden hat „ein wenig Ahnung von dem Thema“ Foto: imago images / Eibner Europa

In jedem Land der Welt sorgt die Sicherheit von Computern dafür, dass Lichter brennen, die Regale gefüllt sind, Dämme nicht brechen und die Logistik wie geschmiert läuft. Seit mehr als einem halben Jahrzehnt wird die Verletzlichkeit von Computern und der Netzwerke, in denen sie hängen, in der „Worldwide Threat Assessment“ der US Intelligence Community als das Risiko Nummer Nummer eins eingestuft – also höher als Terrorismus oder Krieg. Ihr Kontostand, die Ausstattung des örtlichen Krankenhauses und die US-Präsidentschaftswahl 2020 hängen neben vielen, vielen anderen Dingen davon ab, dass Computer sicher sind.

Und obwohl das so ist, versucht die US-Regierung inmitten der größten digitalen Sicherheitskrise der Geschichte zusammen mit den Regierungen Großbritanniens und Australiens, die einzige Methode kalt zu stellen, die derzeit für einen zuverlässigen Schutz von Informationen existiert: die Verschlüsselung. Sollte ihnen das gelingen, würden sowohl unsere öffentliche Infrastruktur als

auch unser Privatleben dauerhaft unsicher.

Im einfachsten Fall ist Verschlüsselung ein Mittel zum Schutz von Informationen, die wichtigste Methode, um Sicherheit für digitale Kommunikation zu gewährleisten. Jede E-Mail, die Sie schreiben, jedes Wort, das Sie in eine Suchmaske eingeben – auch jede Peinlichkeit, die Sie online veranstalten – wird quer durch ein zunehmend feindseliges Internet übertragen. Kürzlich forderten die USA, Großbritannien und Australien Facebook auf, eine „Hintertür" in seinen verschlüsselten Messaging-Apps zu kreieren, die jedem mit dem passenden Schlüssel den uneingeschränkten Zugang auf private Kommunikation ermöglichen würde. Bis dato hat sich Facebook dagegen gewehrt.

Rund um den Globus kippt angesichts der drohenden Klimakatastrophe die Stimmung, und der Protest wird immer lauter. Gleichzeitig sitzt die Welt auf einer 100-Billionen-Dollar-Blase aus Investitionen in fossile Brennstoffe. Zukunftsforscher Jeremy Rifkin zeigt, wie aus dieser Konstellation die einmalige...

Daten nur für die, für die sie bestimmt sind

Wenn der Internetverkehr nicht verschlüsselt wird, kann und wird sich jede Regierung, jedes Unternehmen oder jeder Kriminelle, der das bemerkt, eine Kopie davon ziehen und Ihre Daten für immer speichern. Wenn Sie eben diesen Datenverkehr jedoch verschlüsseln, können Ihre Informationen von niemandem gelesen werden – außer von der Person mit dem passenden Schlüssel.

Ich hab ein wenig Ahnung von dem Thema, da ich eine Zeit lang einen Teil des globalen Systems der Massenüberwachung der NSA mitbetrieben habe. Im Juni 2013 habe ich mich dann mit Journalisten zusammengetan, um dieses skandalöse System ans Licht der Öffentlichkeit zu zerren. Ohne Verschlüsselung hätte ich die Geschichte, wie es dazu kam – mein Buch *Permanent Record* –, nie schreiben können. So aber war es mir möglich, das Manuskript sicher über die Grenzen, die ich selbst nicht mehr überschreiten kann, zu bringen. Viel wichtiger aber ist, dass die Verschlüsselung jedem – von Reportern, Dissidenten, Aktivisten, NGO-Mitarbeitern und Whistleblowern bis hin zu Ärzten, Anwälten und Politikern – hilft, die eigene Arbeit sicher zu verrichten – nicht nur in den gefährlichsten und repressivsten Ländern der Welt, sondern überall.

Als ich 2013 an die Öffentlichkeit ging, überwachte die US-Regierung nicht nur passiv den Verkehr, der durch das Netz waberte – sie hatte Mittel und Wege gefunden, um die internen Netzwerke großer amerikanischer Technologieunternehmen zu kompromittieren und zu infiltrieren. Damals war nur ein kleiner Teil des Webverkehrs verschlüsselt. Sechs Jahre später

haben Facebook, Google und Apple standardmäßige Verschlüsselung zu einem zentralen Bestandteil ihrer Produkte gemacht, so dass inzwischen fast 80 Prozent des Internetverkehrs verschlüsselt sind. Sogar der ehemalige Direktor des nationalen US-Geheimdienstes, James Clapper, gibt zu, dass die Aufdeckung der Massenüberwachung dazu beigetragen hat, die kommerzielle Einführung von Verschlüsselung massiv voranzutreiben. Das Internet ist dadurch sicherer. Für einige Regierungen zu sicher.

Donald Trumps Generalstaatsanwalt William Barr genehmigte eines der frühesten Massenüberwachungsprogramme, ohne zu überprüfen, ob es überhaupt gesetzmäßig ist. Er beabsichtigt nun, die Fortschritte der letzten sechs Jahre in Sachen Verschlüsselung zu stoppen – oder sogar rückgängig zu machen. WhatsApp, der Messaging-Dienst von Facebook, nutzt bereits Ende-zu-Ende-Verschlüsselung (E2EE): Im März kündigte das Unternehmen seine Absicht an, E2EE auch in seine anderen Messaging-Anwendungen – den Facebook Messenger und Instagram – zu integrieren. Daraufhin startete Barr eine öffentliche Kampagne, die verhindern sollte, dass Facebook diese nächste Stufe auf der Leiter der digitalen Sicherheit nimmt. Die Forderung, dass Facebook seine Verschlüsselungspläne aufgeben solle, wurde von einem offenen Brief flankiert, der von Barr, der britischen Innenministerin Priti Patel, Australiens Innenminister und dem US-Minister für innere Sicherheit, mitunterzeichnet wurde.

Hintertüren öffnen Missbrauch Tür und Tor

Sollte die Kampagne von Barr erfolgreich sein, wird die Kommunikation von Milliarden Menschen in einen Zustand permanenter Unsicherheit versetzt. Die Nutzer von Kommunikationsapps würden strukturell verwundbar. Diese von Barr erträumte Art der Kommunikation wird nicht nur für Ermittler aus den USA, Großbritannien und Australien kompromittierbar sein, sondern eben auch für die Geheimdienste Chinas, Russlands und Saudi-Arabiens – ganz zu schweigen von Hackern rund um den Globus.

Ende-zu-Ende-verschlüsselte Kommunikationssysteme sind so konzipiert, dass Nachrichten nur vom Absender und den vorgesehenen Empfängern gelesen werden können. Auch wenn die verschlüsselten – also gesperrten – Nachrichten selbst von einem nicht vertrauenswürdigen Dritten – zum Beispiel einem Unternehmen wie Facebook – gespeichert werden.

Die zentrale Verbesserung, die E2EE gegenüber älteren Sicherheitssystemen bietet, besteht darin, dass die Schlüssel, die eine bestimmte Nachricht entsperren, immer nur an den Endpunkten der Kommunikation, also auf den spezifischen Geräten gespeichert werden. Zum Beispiel auf den Smartphones des Absenders und des Empfängers der Nachricht und eben gerade nicht bei den Internetplattformen selbst. Da E2EE-Schlüssel nicht von diesen zwischengeschalteten Dienstleistern aufbewahrt werden, können sie bei den unterdessen immer

häufiger auftretenden massiven Datengaus dieser Unternehmen nicht mehr gestohlen werden. Für Verbraucher stellt das einen wesentlichen Sicherheitsvorteil dar. E2EE sorgt sozusagen dafür, dass Unternehmen wie Facebook, Google oder Apple ihre Nutzer vor unlauteren Zugriffen eben dieser Unternehmen schützen: Indem sie sicherstellen, dass sie selbst nicht mehr die Schlüssel zu unseren geheimsten Geheimnissen besitzen, werden diese Unternehmen von allsehenden Augen zu Blinden.

Es ist schon bemerkenswert, dass ein für die Privatsphäre von Milliarden von Menschen potenziell so gefährliches Unternehmen wie Facebook zumindest öffentlich bereit zu sein scheint, Technologien einzusetzen, die die eigenen Nutzer sicherer machen, und so seine eigene Macht beschneidet. Noch bemerkenswerter ist es, dass es ausgerechnet die US-Regierung ist, die dann aufjault. Das liegt natürlich allein daran, dass die Regierung so nicht mehr in der Lage wäre, Facebook als einen reichhaltigen Fundus privater Informationen zu behandeln, an dem man sich bequem bedienen kann.

Kriminelle planen ihre Verbrechen nicht auf öffentlichen Plattformen

Um ihr ablehnendes Verhalten gegenüber Verschlüsselungsmethoden zu rechtfertigen, hat die US-Regierung, wie das eben üblich ist, die dunkelsten Kräfte des Netzes heraufbeschworen und den Teufel an die Wand gemalt. Sie behauptet, dass sie ohne uneingeschränkten Zugang zu den vollständigen Aufzeichnungen der Aktivitäten aller Facebook-Nutzer nicht in der Lage wäre, Terroristen, Drogendealer, Geldwäscher und die Täter von Kindesmissbrauch zu verfolgen – Kriminelle, die es in Wirklichkeit natürlich vorziehen, ihre Verbrechen gerade eben nicht auf öffentlichen Plattformen zu planen – insbesondere nicht auf denen in den USA –, da diese mitunter einige der fortschrittlichsten automatischen Filter und Meldemethoden einsetzen.

Die wahre Erklärung dafür, dass die Regierungen der USA, Großbritanniens und Australiens die Ende-zu-Ende-Verschlüsselung abschaffen wollen, hat weniger mit öffentlicher Sicherheit als mit Macht zu tun. E2EE gibt Einzelpersonen und den Geräten, mit denen sie Nachrichten empfangen und verschlüsseln, die Kontrolle – nicht den Unternehmen, die sie bloß weiterleiten. Verschlüsselung bedeutet, dass staatliche Überwachung zielgerichteter und methodischer werden muss. Und nicht willkürlich und universell.

Was die Entwicklung hin zu mehr Endnutzer-Sicherheit gefährdet, ist streng genommen die Fähigkeit von Staaten, ihre Bevölkerung in großem Maßstab auszuspionieren, ohne dass dabei viel bürokratischer Papierkram anfällt. Dadurch dass man die Speicherung von persönlichen Daten und Kommunikation bei Privatunternehmen stark einschränkt, müssen Behörden sich auf klassische Untersuchungsmethoden besinnen, die sowohl effektiv als auch gesetzmäßig sind – im

Gegensatz zur vollständigen Überwachung. Mit Verschlüsselung sind wir nicht nur sicher, sondern auch frei.

Edward Snowden ist ehemaliger CIA-Offizier und Whistleblower. Er ist Autor des Buches *Permanent Record*. Des Weiteren ist er Vorstandsvorsitzender der *Freedom of the Press Foundation*

Übersetzung: Jan Jasper Kosok
15:30 16.10.2019