Linus Neumann

Politische Lösungen für eine sichere Zukunft der Kommunikation

In ihren bisherigen Versuchen, die NSA-Spähaffäre aufzuklären, betreibt die Bundesregierung viel Heimlichtuerei: Zu den technischen Details der amerikanisch/britischen Abhörprogramme könne man nichts sagen; und sofern die Techniken doch bekannt sind (weil deutsche Behörden sie auch nutzen) will man aus Sicherheitsgründen keine Details verraten. Dabei ist die Telekommunikationsüberwachung der beste Beleg dafür, wie sich konspirative Überwachungstechnologien einer transparenten Kontrolle entziehen und tendenziell verselbständigen. Geheime Sicherheitstechnologien sind ein Sicherheitsrisiko, denn ihre Geheimhaltung macht sie selbst anfällig für Angriffe Dritter, die Lücken in den Überwachungssystemen ausnutzen können.

Linus Neumann skizziert in seinem Essay, woher eigentlich die Sicherheitslücken kommen, die Geheimdienste wie Kriminelle für ihre Angriffe auf vertrauliche Telekommunikationen nutzen. Für eine echte Sicherheit sei deshalb ein Wandel der Sicherheitskultur notwendig, der nicht die Geheimhaltung, sondern die öffentliche Kontrolle der zugrundeliegenden Technologien (und Verfahren) zum Leitbild macht. Neben den ganzen politischen wie rechtlichen Gründen für die öffentliche Kontrolle der Staatsgewalt sprechen nach seiner Auffassung auch technische Aspekte dafür, Sicherheit als Aufgabe der Öffentlichkeit zu verstehen und in deren Obhut zu stellen.

Mit der Massenüberwachung durch Geheimdienste und das Bekanntwerden immer neuer, schwerwiegender IT-Sicherheitslücken steigt der Druck auf die Bundesregierung wirksame Schutzmaßnahmen für sichere Kommunikation und Nutzung von Computern durch Bürger_innen und Wirtschaft zu ergreifen.

Dazu ist nötig zu verstehen, wie Sicherheitslücken zustande kommen und wie sie verhindert werden können. Aus diesem Verständnis heraus können die notwendigen politischen Weichenstellungen folgen, die weiter unten vorgestellt werden.

Wie entstehen Sicherheitslücken und welche Typen gibt es?

Der einfache Bug

Die große Mehrheit von Sicherheitslücken in heutigen Software-und Kommunikationssystemen entsteht durch simple Programmierfehler („Bugs“). Die komplexe Logik der Programme bildet sich in Millionen von Zeilen Programmcode ab, die von großen Teams geschrieben werden. Sie alle zu lesen und ihre gegenseitigen Abhängigkeiten und Referenzierungen vollständig zu durchdringen, ist Einzelpersonen kaum möglich. Einzelne Programmteile („Routinen“) der Software verlassen sich auf das korrekte Funktionieren anderer, bestimmte Vorbedingungen werden angenommen, aber an anderer Stelle nicht sichergestellt. So entstehen Bedingungen, die ein/e Angreifer_in durch vom Programm unerwartetes Verhalten auslösen, und so seine Integrität unterwandern kann. Häufig ist der notwendige „Fix“, also die Reparatur des Programms, nur das Löschen oder Hinzufügen einer einzelnen Zeile, wie der inzwischen berühmt gewordenen Zeile „goto fail;“ in *Apples* Implementierung der SSL-Verschlüsselung, die das gesamte Sicherheitsmodell in sich zusammenbrechen ließ.

Backdoors und „Bugdoors“

Oft werden in Programme, Anwendungen und Apps auch absichtliche Hintertüren eingebaut, die den Entwickler_innen oder staatlichen Stellen eine Möglichkeit des Fernzugriffs (also die Umgehung aller Sicherheitsmaßnahmen) bieten sollen. Da immer auch mit dem Entdecken solcher Backdoors gerechnet werden muss, werden diese oft so gestaltet, dass ihre absichtliche Platzierung glaubhaft abzustreiten ist. Äußerlich ähneln sie daher nicht selten versehentlichen Bugs (Programmierfehlern), was den schönen Begriff der „Bugdoor“ geprägt hat.

Absichtliche Design-Schwächen

Insbesondere in Kommunikationssystemen werden Angriffsflächen jedoch häufig schon spezifiziert (geplant), bevor überhaupt eine Zeile Programmcode geschrieben ist: Selbstverständlich ist jeder Telefonanbieter in der Lage, alle Telefonate aller Kund_innen abzuhören und selbstverständlich sind alle E-Mail-Anbieter in der Lage, alle E-Mails aller Kund_innen zu lesen. Das gilt natürlich ebenso für die Sicherheitsbehörden, mit denen der Anbieter kooperiert, wie für staatliche Stellen oder kriminelle Angreifer_innen, die den Anbieter unterwandern. Da die Massenüberwachung möglich ist, findet sie auch statt.

Doch das muss nicht so sein: Kommunikationssysteme, die ihre Nutzer_innen auch vor dem Zugriff durch den Mail- oder Telekommunikationsanbieter schützen, sind zwar möglich, aber ihre Verbreitung von keiner Regierung dieser Welt wirklich

gewünscht. Zu groß ist die Sorge, allen Menschen ein nicht überwachbares Kommunikationsmittel zur Verfügung zu stellen und die eigenen und freundschaftlich verbundenen Geheimdienste in ihrer Überwachung zu beschränken.

Das System De-Mail, als „sichere Alternative zur E-Mail“ beworben, ist hierfür das beste Beispiel: Nicht nur bietet es keine sichere Verschlüsselung, es wurde zudem unter Beteiligung der selben US-amerikanischen Firma entwickelt, die auch an der Entwicklung des Staatstrojaners beteiligt ist und in den USA einer der größten Zulieferer der NSA ist: der *Computer Sciences Corporation*, kurz CSC.

Sichere Kommunikation braucht politische Lösungen

Um eine verlässliche und sichere Kommunikation zu ermöglichen, müssen alle drei Arten von Sicherheitslücken eingedämmt werden: unabsichtliche Bugs, absichtliche Backdoors und schon im Design eingeplante Schwächen. Hierzu gibt es mehrere Ansätze, die eine Politik, die IT-Sicherheit und sichere Kommunikation fördern will, umsetzen sollte:

1) Open-Source-Software fördern

Das Finden von Bugs und Backdoors ist eine sehr mühselige Arbeit, die enorm erleichtert wird, wenn nicht erst das fertige Programm geprüft, sondern sein zugrundeliegender Programm-Quelltext gelesen werden kann. Nur bei einer Software, deren vollständiger Quelltext offen liegt, besteht überhaupt die Basis für ein Vertrauen in deren Integrität. Denn wie wir alle wissen, ist Vertrauen gut, aber Kontrolle besser. Genau diese öffentliche Kontrolle verweigern jedoch die meisten kommerziellen Anbieter, da sie das Abfließen ihrer Entwicklungen an die Konkurrenz fürchten: Wer den Quelltext hat, kann die Software weiterentwickeln, verbessern oder verändern. Das wäre zwar im Interesse der Allgemeinheit, nicht jedoch im Interesse des Anbieters.

Hier gilt es, einerseits kommerzielle Anreize zur Open-Source-Entwicklung zu bieten, andererseits entsprechende Bedingungen für die Anbieter von sicherheitsrelevanter Software zu setzen: Auch heute noch operieren sie größtenteils frei von jeglicher Haftung für ihr intransparentes Produkt, und somit ohne Anreiz zur nennenswerten Qualitätssicherung.

2) Den Schwarzmarkt trockenlegen

Wer mit seiner Fähigkeit zum Finden von Sicherheitslücken den Lebensunterhalt bestreiten möchte, dem bieten sich heute zwei Möglichkeiten:

Ein solides mittelständisches Auskommen hat, wer als Dienstleister_in Sicherheitsprüfungen bei Dienstanbietern und Software-Schmieden durchführt und sich im

Anschluss an seine Untersuchung den bürokratischen und firmenpolitischen Diskussionen um die Behebung der entdeckten Probleme stellt.

Wer ethisch flexibler ist, dem winken auf dem Schwarzmarkt sechsstellige Beträge für das Finden von großen Sicherheitslücken in weit verbreiteter Software. Die fürstliche Entlohnung entschädigt für die Gewissensbisse, weil die entdeckte Lücke künftig nicht geschlossen, sondern von Kriminellen und/oder Geheimdiensten ausgenutzt wird. Letztere sind dabei die treibende Kraft hinter den hohen Preisen auf diesem moralisch verwerflichen Markt.

Hier gilt es, einen Riegel vorzuschieben: Die staatliche Subventionierung des Schwarzmarkts muss unterbunden und alle staatlichen Stellen müssen verpflichtet werden, beim Bekanntwerden von Sicherheitslücken kompromisslos auf ihre Beseitigung hinzuarbeiten – und nicht auf ihre Ausnutzung.

3) Eine offene Sicherheitskultur pflegen

Natürlich werden Sicherheitslücken nicht nur wegen kommerzieller Anreize entdeckt. Eine weltweite Community begeisterter Hacker, Nerds und Sicherheitsforscher_innen sucht, findet und beseitigt Sicherheitslücken ohne direkte monetäre Kompensation. Namentliche Erwähnungen in „Security Bulletins“, die Nutzer_innen auf Lücken und erhältliche Updates hinweisen, sind oft der einzige Dank, der ihnen für ihre Dienste an der Gemeinschaft zuteil wird.

Immer beliebter wird daher das Ausloben von „Kopfgeld“ („Bug Bountys“) auf Sicherheitslücken in kritischer Open-Source-Software: Wer einen Fehler definierter Schwere findet, wird dafür entlohnt. Vom entstehenden Wettkampf der Forschenden profitiert die Allgemeinheit. Um dies zu stärken, könnte das Bundesamt für Sicherheit in der Informationstechnik (BSI) sich an der Finanzierung dieser „Bug Bountys“ beteiligen und so Open-Source-Software sicherer machen.

4) Eine unabhängige Sicherheitspolitik ermöglichen

Mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) verfügt die Bundesregierung über eine Institution, die aktuell viele Möglichkeiten ungenutzt lässt, auf den überfälligen Paradigmenwechsel in der IT-Sicherheit hinzuwirken. Dem Verantwortungsbereich des Innenministeriums unterliegend, kann das BSI in seinen Empfehlungen, Spezifizierungen und Zertifizierungen nie wirklich frei agieren. Das mit einer staatlichen Abhörschnittstelle versehene und zusammen mit einem NSA-Dienstleister entwickelte De-Mail-System ist mit Fug und Recht zur Blamage für das BSI geworden.

Solange das BSI dem Innenminister untersteht, ist trotz aller Lippenbekenntnisse nicht damit zu rechnen, dass dort künftig Spezifikationen ohne absichtliche Design-Schwächen entwickelt werden. Ein starkes, unabhängiges BSI mit unzweideutigem Sicherheitsauftrag – und zwar auch gegen staatliche Angreifer – ist der einzige Weg,

das notwendige Vertrauen im Bereich der IT-Sicherheit aufzubauen und Sicherheitsversprechen auch halten zu können.

2008 formulierte das Bundesverfassungsgericht das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, das so genannte Computergrundrecht. Bisher haben staatliche Stellen nur halbherzige und unglaubwürdige Schritte zu seiner Sicherung unternommen. Das schockierende Ausmaß der Snowden-Enthüllungen ist eine direkte Folge der bisherigen Politik und ein weiteres Warnsignal an die Bundesregierung, die Sicherheit der Bürgerinnen und Bürger in Sachen Computernutzung und Kommunikation nicht unnötig der vermeintlichen Sicherheit des Staates zu opfern.

LINUS NEUMANN ist Diplompsychologe und arbeitet bei einem Unternehmen zur IT-Sicherheit in Berlin. Er ist Mitglied des Chaos Computer Clubs und vertritt diesen als Sachverständiger. Darüber hinaus gehört er seit 2010 zur Redaktion von netzpolitik.org und erstellt gemeinsam mit Tim Pritlove den wöchentlichen Podcast „Logbuch: Netzpolitik“.