2015/48 Lifestyle

https://www.jungle.world/artikel/2015/48/kein-schluessel-nirgends

Die digitale Kommunikation der Atttentäter von Paris war nicht verschlüsselt

Kein Schlüssel, nirgends

Von **Boris Mayer**

Die Attentäter von Paris kommunizierten unverschlüsselt und nicht über geheime Netzwerke. Dass die Anschläge nicht verhindert werden konnten, liegt unter anderem an der unfassbaren Menge an Daten, die im Internet unterwegs sind.

Nach den Terroranschlägen von Paris wird unweigerlich die Frage gestellt: Wie konnte das nur passieren und wieso haben die Geheimdienste die Anschläge nicht vorher vereitelt oder wenigstens vor ihnen gewarnt? Eine gute Frage; das Problem ist nur, dass die meisten Antwortversuche von Menschen kommen, die eine eigene Agenda haben.
Bereits während der jüngsten Terrorattacken in Paris war klar, dass die üblichen Verdächtigen die Situation dazu nutzen würden, die Aufnahme von syrischen Flüchtlingen in Deutschland anzuprangern. Ebenso unvermeidlich war, dass Geheimdienstsprecher und ihnen nahestehende Politiker die Verschlüsselung der digitalen Kommunikation für die mangelnde Informationslage bei CIA, BND & Co. verantwortlich machen würden. Auch verwunderte es kaum, dass man Edward Snowden vorwerfen würde, seinetwegen wüssten die Terroristen nunmehr, welche Daten die Spähprogramme erfassen können, und könnten diese deshalb meiden. Genauso vorhersehbar wie die Behauptungen, Snowden und die Kryptographie seien für das Versagen der Geheimdienste mitverantwortlich, waren allerdings auch die Reaktionen auf diese Behauptungen. Es sei ungeheuerlich, überhaupt darüber nachzudenken, die Privatsphäre weiter aufzuweichen, empören sich Netzaktivisten regelmäßig und merken an, dass es keinesfalls eine Lösung sei, Kryptographie zu verbieten oder staatlich zu regulieren.
Dass Staaten die Kryptographie kontrollieren wollen, ist nicht neu. Bereits die erste Version der Verschlüsselungssoftware »Pretty Good Privacy« (PGP) brachte deren Entwickler, Phil Zimmerman, 1993 Ermittlungen wegen unerlaubten Waffenexports ein, die erst nach drei Jahren ohne Ergebnis endeten. Zimmermann hatte die Exportbestimmungen für Kryptosoftware umgangen, indem er den Quellcode als Buch veröffentlichte, so konnte das Buch in anderen Ländern gekauft, abgetippt und kompiliert werden.
Ernsthaft auf Kryptographie verzichten möchte heute niemand mehr, sei es beim Onlinebanking oder auch nur bei der Übertragung von Passwörtern für so ziemlich jeden

einzelnen Dienst im Internet. Auch das Bundeswirtschaftsministerium hat bereits einige Kampagnen lanciert, die Unternehmen die Wichtigkeit von Verschlüsselung als Instrument gegen Wirtschaftsspionage erklären sollten. Die Forderung, Kryptographie so zu regeln, dass staatliche Stellen einen Zweitschlüssel erhalten, wurde bereits nach den Anschlägen vom Januar diskutiert. Sie zeugt von Unkenntnis, denn die Sicherung eines solchen Systems wäre schlichtweg unmöglich. Ein Schlüssel, der alle Schlösser öffnet, hebelt schließlich jegliche Sicherheit aus, mit unabsehbaren Folgen, wenn er in die Hände Unbefugter gelangen würde. Selbst das FBI hält ein System solcher Zweitschlüssel für technisch nicht realisierbar und bezeichnet es als Wunschdenken.

Dass die Geheimdienste die Morde in Paris nicht verhindern konnten, hat ganz andere Gründe, und diese haben nichts mit Kryptographie zu tun, wie im Grunde jeder, der auch nur etwas Wissen über Datenverkehr, Data-Mining und das Internet hat, erkennen kann. So ist inzwischen bekannt, dass die Attentäter von Paris größtenteils unverschlüsselte SMS zur Koordinierung der Anschläge nutzten. Genauso stellte sich die unmittelbar nach den Taten angeprangerte Verwendung des Messaging-Dienstes Telegram als unverschlüsselte Verbreitung von Propaganda heraus: Der Dienst wurde nicht als Planungsplattform genutzt.
Telegram wurde übrigens von zwei Exilrussen entwickelt, die vorher das russische soziale Netzwerk vk.com betrieben hatten. Sie wollten damit sichere Kommunikation ermöglichen, ein Wunsch, der nach den Erfahrungen mit ihrem sozialen Netzwerk naheliegt. Die Kontrolle über vk.com verloren die Entwickler nämlich an Wladimir Putin nahestehende Geschäftsleute, als sie sich weigerten, Accounts von Oppositionellen und ukrainischen Demonstranten zu sperren, wie es die russische Regierung gefordert hatte.
Die Terroristen sollen über Whatsapp und weitere Dienste kommuniziert haben und unterschieden sich in ihrem Verhalten damit kaum von anderen Internetbenutzern. Verschlüsselung sei ihnen offenbar nicht so wichtig gewesen, wie Politik und Geheimdienste die Öffentlichkeit zunächst glauben machen wollten.
Ein viel größeres Problem als die Verschlüsselung ist die Menge der Daten, die im Internet unterwegs sind. Allein bei Twitter waren es schon vor zwei Jahren 500 Millionen Tweets am Tag – inzwischen ist die Zahl der User um 40 Prozent gestiegen. Überwachungsrelevant sind in diesem Zusammenhang allerdings nicht nur die Kurznachrichten, sondern auch die sozialen Verknüpfungen von Usern sowie deren Nutzerverhalten. Twitter ist nur einer von vielen Diensten, die irgendeine Form von Text, Sprache, Bilderverbreitung oder Videoeingabe erlauben, die andere Internetnutzer sehen können. Dazu kommen E-Mail-Dienste, Chatprogramme sowie Telefonie mit oder ohne Video.
Wenn also Geheimdienste den Großteil dieses Datenverkehrs mitschneiden und auswerten, kann dies nur unter Verwendung von automatischen Suchmustern erfolgen. Man braucht ein Muster, das möglichst alle Terrorpläne aufdeckt, gleichzeitig aber nicht gleich Alarm schlägt, nur weil jemand buzzwords wie »Jihad« erwähnt. Dass diese Aufgabe nicht so einfach zu bewältigen ist, kann jeder Internetnutzer am eigenen E-Mail-Postfach immer wieder feststellen: Auch nach 20 Jahren permanenter Weiterentwicklung funktioniert die automatisierte Unterscheidung von Spam und relevanten E-Mails nicht einmal annähernd einwandfrei.
Geheimdienste versuchen, in einem Misthaufen ungeheurer Dimensionen einzelne Informationen zu finden, die ihnen dann eventuell Anhaltspunkte für weitere Recherchen

geben. Aber allein die Zahlen, die den Internet-Datenverkehr betreffen, sind unfassbar. Nach Angaben von Cisco, dem führenden Hersteller für Internet-Backbone-Technik, wird der Datenverkehr im Internet im Jahr 2016 erstmals die Zettabyte-Grenze überschreiten. Das bedeutet einen monatlichen Datenverkehr von über 88 Exabytes. Ein Exabyte sind eine Milliarde Gigabyte. Zum Vergleich: Das Print-Archiv der US-amerikanischen Library of Congress würde 100 000 Mal in ein Exabyte passen. Die Datenmenge ist also unvorstellbar groß. Das führt zu Informationsüberflutung, auch infoxication genannt. Denn es reicht nicht, nach einzelnen Stichworten zu suchen. Wichtig sind auch die Metadaten, wer mit wem kommuniziert, was ausgetauscht wird und wie das alles mit der Kommunikation der beteiligten Personen in der Vergangenheit zusammenhängt. Diese Analyse muss bewertet werden, um dann eine Nachverfolgung durch weitere Filter oder eben auch durch menschliche Analysten zu ermöglichen.

Dass bei diesem Eindampfen von Daten auf ein erträgliches Maß manch wichtiger Hinweis durch das Sieb fällt oder ein Zusammenhang nicht erkannt wird, ist unvermeidlich. Denn um die Daten auszuwerten, müssen die Computersysteme der Geheimdienste sie erst einmal verstehen. Die Erkennung von Sprache oder Text wurde in den vergangenen Jahren zwar deutlich verbessert, und die Geheimdienste dürften bei ihren Filtern bessere Software zur Verfügung haben als der einzelne PC- oder Handy-Nutzer. Aber wenn Text- und Spracherkennung einfach zu optimieren wären, würde die Tastatur des Smartphone schon lange nur noch richtige Korrekturvorschläge machen, die Autokorrektur der Textverarbeitung nicht mehr für absurde Vorschläge sorgen und der Apple-Sprachassistent Siri alles sofort richtig verstehen. Und dabei wird dem Handy, der Textverarbeitung oder der Spracherkennung vorher angesagt, in welcher Sprache die Kommunikation stattfinden wird. Das steht im Gegensatz zur menschlichen Kommunikation, in die ansatzlos Redewendungen oder Wörter in einer ganz anderen Sprache einfließen können, was die automatisierte Überwachung zusätzlich erschwert.
Der Cyberwar wird nicht dadurch erschwert, dass die Terroristen sich ins Darknet zurückziehen und Verschlüsselungstechnik benutzen, sondern dadurch, dass es fast unmöglich ist, die wenigen relevanten Daten aus einer riesigen Menge herauszufischen. Das zeigt auch eine offizielle Studie des Thinktanks »New America Foundation« im Januar 2013. Sie stellte fest, dass mit Hilfe der Datensammlung der NSA bis zu jenem Zeitpunkt genau null Anschläge verhindert werden konnten. Insgesamt wurden 17 Ermittlungsverfahren eingeleitet, von denen ein einziges zu einer Verurteilung führte: Ein Taxifahrer hatte einer terroristischen Gruppe in Somalia Geld geschickt.
Noch etwas zeigt, dass nicht hochverschlüsselte Kommunikationswege und große Technologie-Expertise der Terroristen der Grund waren, dass die Anschläge von Paris nicht verhindert werden konnten: Nach den Morden standen die Identitäten der Jihadisten als Ansatzpunkt zur Verfügung. Es dauerte auch nicht mehr lange, bis Komplizen und Drahtzieher identifiziert werden konnten. Die relevanten Daten waren nicht verschlüsselt, aber eben erst durch die Tat auffindbar.