SWP-Aktuell

Stiftung
Wissenschaft und
Politik

Deutsches Institut
für Internationale
Politik und Sicherheit

Verschlüsselung in Gefahr

Weltweit schwächen Staaten die Cyber-Sicherheit – Deutschland sollte dagegenhalten

Matthias Schulze

Gegenwärtig formiert sich weltweit eine unfreiwillige Allianz von Gegnern der Verschlüsselung. Neben autoritären Regimen setzen auch immer mehr westliche Demokratien darauf, die Kommunikationsverschlüsselung zu schwächen und Spionage-Software auf Smartphones zu nutzen. Damit wird ein globaler Normsetzungsprozess beschleunigt, der die Bemühungen um Cyber-Sicherheit konterkariert. Deutschland sollte sich diesem Trend entgegenstellen und seine Ambitionen als Verschlüsselungsstandort Nummer eins verstärken. Dabei gilt es auch, alternative Ermittlungswege zu finden, damit Terrorverdächtige von Behörden überwacht werden können, ohne dass die Software-Sicherheit der ganzen Bevölkerung leidet.

Verschlüsselungstechnologien sind ein zweischneidiges Schwert. Einerseits ist Verschlüsselung im digitalen Zeitalter unabdingbar, etwa für Online-Banking (SSL/TLS), zum sicheren Websurfen (HTTPS) oder beim Umgang mit sensiblen Daten. Sie bietet einen wesentlichen Schutz sowohl vor Cyber-Kriminellen als auch vor fremden Nachrichtendiensten. Andererseits kann Verschlüsselung auch Kriminellen dazu dienen, Kommunikation vor Strafverfolgungsbehörden zu verschleiern. Dieses Dilemma ist seit mehr als zwei Dekaden immer wieder Gegenstand politischer Debatten. Die US-Regierung erwog in den 1990er Jahren ein Verbot der Verschlüsselung und forderte den Einbau staatlicher Hintertüren in Computerchips, um verschlüsselte Kommunikation mitlesen zu können (»Crypto Wars«). Zivilgesellschaftlicher Widerstand – zusammen mit technischen Hürden – führte schließlich zu dem allgemeinen Konsens, dass mehr Verschlüsselung eine digitalisierte Welt sicherer macht.

Dieser Konsens scheint sich gegenwärtig aufzulösen. Sei es aus Angst vor Terrorismus oder aus Gründen der Zensur – immer mehr Staaten suchen nach Wegen, um Verschlüsselung zu umgehen, etwa durch das Ausnutzen von Software-Schwachstellen. Da neuerdings neben autoritären Regimen auch demokratische Rechtsstaaten diesem Pfad folgen, droht sich hier eine neue internationale Norm zu etablieren. Deutschland sollte sich dem Trend entgegenstellen, denn Software-Schwachstellen gefährden die Cyber-Sicherheit der Bevölkerung, laden zu Missbrauch ein und sind bei der Terrorismusbekämpfung nur begrenzt wirksam.

Matthias Schulze ist Wissenschaftler in der SWP-Forschungsgruppe Sicherheitspolitik

China und Russland

Im Januar 2017 führte die chinesische Regierung eine staatliche Lizenzpflicht für die Nutzung sogenannter Virtual Private Network Software (VPN) ein. Rund 90 Millionen Chinesen nutzen VPN-Clients, die die gesamte Internetkommunikation verschlüsseln. Auf diese Weise lässt sich die Infrastruktur umgehen, die Peking zur Überwachung und Zensur des Internets einsetzt (»Great Firewall«). Möglich wird ein Zugriff auf westliche, unzensierte Dienste wie etwa Wikipedia. Staatlich lizenzierte VPN-Dienste hingegen würden ebenjene Überwachungs- und Zensurfilter beinhalten, die eigentlich umgangen werden sollen. Für Missachtung sieht die Regelung hohe Strafen vor. Westliche Unternehmen, die in China tätig sind, wurden kürzlich verpflichtet, ihre Dienste auf chinesische VPNs umzustellen. Apple beugte sich dem Druck Pekings und entfernte westliche VPN-Clients aus dem iOS-App-Store.

Initiativen zur staatlichen Kontrolle von VPN-Clients gibt es ebenso im Iran und in Syrien sowie neuerdings auch in Russland. Das russische Unterhaus beschloss im Juli 2017 ein Gesetz, das es verbietet, VPN-Clients und das Anonymisierungsnetzwerk TOR zu nutzen, solange diese Dienste keine staatliche Zensur und Internetüberwachung (SORM-II) implementieren. Bereits im Juli 2016 wurde ein russisches Anti-Terror-Gesetz verabschiedet, das unter anderem eine erweiterte Vorratsdatenspeicherung umfasst und Firmen verpflichtet, staatliche Hintertüren in verschlüsselte Dienste einzubauen. Anbieter wie Telegram oder WhatsApp sind so gezwungen, russischen Sicherheitsbehörden die Schlüssel für die Kommunikation zu übergeben oder die verborgenen Inhalte anderweitig bereitzustellen.

Großbritannien, Australien, USA

Solche drastischen Maßnahmen ergreifen aber nicht nur autoritäre Regime. In Großbritannien wurde 2016 die Investigatory Powers Bill verabschiedet, die Regelungen für eine staatlich mandatierte Verschlüsselung enthält. Das Gesetz zwingt Internetdienstleister dazu, Verschlüsselungsmaßnahmen bei Anordnung aufzuheben. Firmen können verpflichtet werden, in ihre Produkte unsichere Hintertüren für geheimen staatlichen Zugriff einzubauen, Überwachungssoftware auf Geräte der Kunden aufzuspielen oder Sicherheits-Updates zu blockieren. Wie dies von internationalen Unternehmen eingefordert werden soll, ist unklar, weshalb die Maßnahmen bisher noch nicht umgesetzt wurden. Trotz solcher Schwierigkeiten plant Australien gerade ein sehr ähnliches Gesetz. Der aktuelle Entwurf sieht vor, dass von WhatsApp und Co. verlangt werden kann, den Strafverfolgungsbehörden verschlüsselte Kommunikationsinhalte zugänglich zu machen.

In den USA sieht die – bislang nicht verabschiedete – Burr-Feinstein Encryption Bill von 2016 vor, dass Unternehmen die (Cyber-)Sicherheit ihrer Produkte absichtlich senken sollen, um Behörden leichteren Zugang zu verschlüsselter Kommunikation zu ermöglichen. Ferner könnten Firmen auf Richterbeschluss gezwungen werden, Daten für Behörden zu entschlüsseln. Der Gesetzentwurf entspricht einer Forderung der Bundespolizei FBI, die Sicherheitsmechanismen im Apple-Betriebssystem iOS zu senken. Das FBI wollte 2016 das verschlüsselte iPhone des Attentäters von San Bernardino hacken, scheiterte aber an den hohen Cyber-Sicherheitsstandards der Software.

Die genannten Bemühungen stehen im Kontext einer Initiative der »Five Eyes«-Geheimdienstpartnerschaft zwischen den USA, Kanada, Großbritannien, Australien und Neuseeland. Ziel ist ein globales Regime, mit dem verhindert werden soll, dass Terroristen verschlüsselte Kommunikation nutzen. Die Initiative ist kompatibel mit den Interessen Chinas und Russlands, treibt also einen globalen Normsetzungsprozess im Cyberspace voran. Ein Kommuniqué der Five Eyes von Juni 2017 sieht gemeinsame Maßnahmen vor, die legalen Zugang zu verschlüsselter Kommunikation ermöglichen. Die Staaten wollen dabei mit der IT-Industrie kooperieren, blenden praktische Prob-

leme aber aus. Hersteller wie Apple, Google und Microsoft haben sich in der Vergangenheit immer wieder dagegen gewehrt, ihre Systeme absichtlich zu schwächen.

Deutschland

Die Position Deutschlands ist widersprüchlich. In ihrer Cyber-Sicherheitsstrategie von 2016 betonte die Bundesregierung den Nutzen von Verschlüsselung etwa bei digitalen Behördengängen und E-Commerce (»Sicherheit durch Verschlüsselung«), wies aber zugleich auf Gefahren hin (»Sicherheit trotz Verschlüsselung«). Die Digitale Agenda von 2014 will Deutschland gar zum Verschlüsselungsstandort Nummer eins machen. Behörden wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) wenden sich seit langem gegen staatliche Hintertüren oder eine Schwächung von Verschlüsselung für Strafverfolgungszwecke.

Doch deutet sich mittlerweile eine Abkehr von einer starken deutschen Cyber-Sicherheitspolitik an. Dies zeigt das BKA-Gesetz von Juni 2017, das den Einsatz von Überwachungstrojanern auf Endgeräten wie Smartphones legitimiert, oder die Gründung der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS), die ebenjene Überwachungslösungen entwickeln soll. Während die Verschlüsselungssoftware technisch unangetastet bleibt, soll stattdessen die Kommunikation auf den Endgeräten *vor* der Verschlüsselung mittels staatlicher Überwachungssoftware ausgelesen werden.

Nationale Sicherheit versus Cyber-Sicherheit

Das Hacken von Smartphones ist mit hohen Kosten verbunden. Berührt werden dabei nicht nur Fragen der Privatsphäre – die Artikel 10 des Grundgesetzes schützt – und das Recht auf die Vertraulichkeit von Informationssystemen, wie es 2008 das Bundesverfassungsgericht formuliert hat. Es geht ebenso um die Standards der allgemeinen Cyber-Sicherheit.

In der IT-Community besteht weltweit Einigkeit, dass es technisch unmöglich ist, einen exklusiven Zugang für Strafverfolgungsbehörden zu gewährleisten, ohne die Sicherheit von Produkten insgesamt zu reduzieren. Bei gängigen Verschlüsselungsverfahren können nur autorisierte Nutzer (Sender und Empfänger) Nachrichten entschlüsseln, nicht aber Dritte (Hacker, Behörden). Die Verschlüsselung stellt also nicht nur sicher, dass Kommunikation weder abgehört noch im Transit manipuliert wird (Vertraulichkeit & Integrität), sondern auch, dass die Kommunikationspartner jene sind, die sie vorgeben zu sein (Authentizität). Neuere Verfahren sehen zudem die Verwendung von Einmal-Schlüsseln (»forward secrecy«) oder die Generierung von Schlüsseln auf sicheren Chips in den Geräten der Kunden vor. IT-Dienstleister sind so technisch gar nicht in der Lage, Behörden die Schlüssel zu übergeben oder die Kundenkommunikation zu entschlüsseln.

Technisch ist es nur noch möglich, Kommunikation zu überwachen, bevor sie verschlüsselt wird. Dies erfordert »hacks« bzw. den Einsatz von spezieller Schad- oder Überwachungssoftware, die aber Sicherheitsmechanismen auf den Geräten schwächt oder ausschaltet. Bewusst platzierte oder tolerierte Schwachstellen in Software werden aber auch von Cyber-Kriminellen und gegnerischen Geheimdiensten ausgenutzt.

In der Konsequenz entsteht ein Dilemma: Entweder man senkt die Cyber-Sicherheit von IT-Produkten, um Terrorverdächtige zu überwachen, womit man gleichzeitig mehr Hacking und Datendiebstahl riskiert, oder man nimmt in Kauf, dass bestimmte Kriminelle nicht mehr so einfach elektronisch zu überwachen sind. Durch Hacking und Cyber-Angriffe entstehen immense Schäden; nach Schätzungen belaufen sie sich auf jährlich bis zu 500 Milliarden US-Dollar. Daher meint etwa James Clapper, ehemals oberster US-Geheimdienstkoordinator, dass Cyber-Sicherheit das dominierende Gut für die nationale Sicherheit sei – angesichts einer eher geringen Wahrscheinlichkeit von Terroranschlägen.

SWP
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 3–4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN 1611-6364

Die Kosten einer Schwächung von Software sind also hoch, während der Nutzen wohl eher gering ist. Terroristen verwenden in der Regel keine Dienste, die von staatlicher Seite überwacht werden können. Gilt eine Technologie als kompromittiert (wie etwa Skype seit 2008), werden Kommunikationskanäle gewechselt. Leitfäden des »Islamischen Staates« empfehlen neben der Verwendung von Wegwerf-Handys oder Smartphones mit multiplen SIM-Karten (für mehrere WhatsApp- oder Telegram-Accounts) den Einsatz nichtpermanenter Betriebssysteme wie Tails. Dies mindert die Effektivität von Überwachungstrojanern. Zu erwarten ist, dass Kriminelle durch mandatierte Schwachstellen etwa in Smartphone-Software zu noch schwerer überwachbaren Technologien getrieben werden, während die Smartphones der Bevölkerung bewusst unsicher gehalten werden. Letzteres ist fahrlässig, zumal die Zahl der Cyber-Sicherheitsvorfälle steigt und davon immer mehr Nutzer betroffen sind. Kürzlich befiel etwa die Schadsoftware »WannaCry« weltweit Hunderttausende Rechner, und in Mexiko fand man den Überwachungstrojaner »Pegasus« auf den Smartphones vieler Journalisten, Anwälte und Aktivisten.

Aktuelle Entwicklungen wie das Internet der Dinge oder der Trend zum mobilen Arbeiten verändern die Rolle von Smartphones. Diese sind immer weniger Kommunikationsgeräte und immer mehr Steuerungsapparate für den Alltag. Sie verwalten Konten und digitale Geldbörsen, öffnen elektronische Haustüren – und sind elementar für die Cyber-Sicherheit, etwa zur Zwei-Faktor-Authentifizierung von Online-Services. Das Kompromittieren von Smartphones mit Trojaner-Software, die unter Umständen auch von Hackern und Geheimdiensten gekapert werden kann, unterminiert die Sicherheit aller Dienste, die mit dem Smartphone verbunden sind. Hinzu kommt das Problem der Signalwirkung. Wenn liberale Demokratien zur Terrorbekämpfung zunehmend Software und Verschlüsselung schwächen, dann legitimiert dies ähnliche Praktiken autoritärer Staaten.

Lösungsvorschläge

Angesichts der globalen Initiativen von Geheimdiensten und autoritären Regimen sollte Deutschland noch nachdrücklicher für sichere Software und Verschlüsselung plädieren. Es gilt zugleich, Allianzen mit anderen demokratischen EU-Staaten zu stärken, damit sich der globale Normsetzungsprozess gegen Verschlüsselung stoppen lässt. Da staatlich mandatierte Software-Schwachstellen die allgemeinen Bemühungen um Cyber-Sicherheit konterkarieren, sollten neue Ermittlungstechnologien und -strategien erforscht werden.

Eine unabhängige wissenschaftliche Kommission sollte prüfen, wie groß das Problem nicht knackbarer Verschlüsselung tatsächlich ist. Jenseits der üblichen Rufe nach mehr staatlichen Befugnissen, die meist nur auf anekdotischer Evidenz basieren, gibt es kaum verlässliche Daten darüber, in wie vielen Fällen Ermittlungen eingestellt werden mussten, weil Smartphones nicht überwacht werden konnten. Ferner ist in den bekannten Fällen oft unklar, ob es nicht alternative Wege gegeben hätte, an Kommunikationsdaten zu gelangen.

Eine solche Kommission könnte sich auch damit befassen, neue Ermittlungsstrategien zu entwickeln. Seit 2001 haben Staaten auf technische Überwachungskapazitäten gesetzt, dabei aber immer mehr Personal eingespart. Zu prüfen wäre, inwiefern personalintensive Verfahren sinnvoll und rechtlich angemessen sind. Cyber-Crime-Ermittlungen im Darknet sind ein gutes Beispiel. Illegale anonyme Marktplätze wie Hansa oder AlphaBay ließen sich ausheben, weil die Täter Fehler begingen oder Ermittler geschickte Fallen aufstellten, um Passwörter zu entlocken. Bei Hansa führte eine Hausdurchsuchung zum Zugriff auf den verschlüsselten Steuerungsrechner des Täters. Alternativ ließen sich Smartphone-PINs während der Eingabe per Fernobservation ermitteln. Solche Maßnahmen würden einen legitimen Zugriff des Staates auf verschlüsselte Kommunikation von Kriminellen gewährleisten, ohne die Cyber-Sicherheit der Bürger insgesamt zu senken.