Schutz der Privatsphäre durch Verschlüsselung und Anonymisierung

Wichtige Schutzmaßnahmen

> »Verschlüsselung ist die wichtigste Technologie zum Schutz der Privatsphäre. (Bruce Schneier)«[1]

> »Verschlüsselung und Anonymität, getrennt oder zusammen, schaffen eine Zone der Privatheit zum Schutz von Meinung und Überzeugung.«[2]

Verschlüsselung und Anonymisierung sind die wichtigsten Hilfsmittel, die wir haben, um unsere Kommunikation und unsere Daten vor unberechtigten Zugriffen zu schützen. Auch wenn es keinen hundertprozentigen Schutz gibt, so kann man damit den unbefugten Zugriff zumindest erheblich erschweren.

Je mehr unser Leben im digitalen Raum stattfindet, desto wichtiger werden Werkzeuge für die Kommunikationssicherheit wie Verschlüsselung und Anonymisierung, für den Schutz der Menschenrechte – insbesondere für das Recht auf Privatheit und für das Recht auf freie Meinungsäußerung. Werkzeuge für die Kommunikationssi-

1 »Encryption is the most important privacy-preserving technology we have. (Bruce Schneier)«. Crowe, A./Lee, S. and Verstraete, M. 17. Juni 2015.

2 »Encryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief.« Encryption and Anonymity create »a zone of privacy online«, says UN Special Rapporteur 2015.

cherheit geben Menschen Zugang zu sicheren und privaten Räumen für ihre persönliche Entfaltung, wo sie ohne unbefugte Einmischung kommunizieren können.[3]

Leider lassen neueste Untersuchungen den Schluss zu, dass Anonymisierung mithilfe Künstlicher Intelligenz und maschinellen Lernens ausgehebelt werden kann. Die derzeit verwendeten Verfahren zur Anonymisierung bieten nicht den versprochenen Schutz der Daten.[4]

> »Verschlüsselung und andere Schutzmaßnahmen (z.B. Zeitverzögerungen bei der Eingabe falscher PINs) sichern unsere Systeme und sollten niemals untergraben werden.«[5]

> »Der Kampf um die Verschlüsselung […] dreht sich im Kern um Freiheit und Unabhängigkeit.«[6]

Doch so wichtig heute Verschlüsselung ist, wird sie doch im Privatbereich nur von vergleichsweise wenigen eingesetzt. Zwar kann in den meisten westlichen Ländern jeder Verschlüsselung einsetzen, doch vielen fehlt das technische Know-how und das Wissen um die Bedeutung von Verschlüsselung. Zudem gilt, dass wir von Verschlüsselung

3 »As more of our lives are lived in the digital realm, communication security tools, such as encryption and anonymity tools and services, are increasingly important to the protection of human rights – particularly the right to privacy and the right to freedom of expression. Communication security tools give individuals access to safe and private spaces for personal development where they can communicate without unwarranted interference.« Anna Crowe, Sarah Lee and Mark Verstraete. (17th June 2015). Securing Safe Spaces Online. Abgerufen am 15. November 2020 von https://privacyinternational.org/sites/default/files/2018-02/Securing %20 Safe %20Spaces %20Online_2_0.pdf.

4 Vgl. Michaels 2019; Hern 2019.

5 »Encryption and other protections (such as time delays as incorrect PINs are entered) secure our systems, and should never be undermined.« Landau 2016.

6 »The fight about encryption, Landau said, ›is, at its core, about freedom and liberty‹.« Landau 2017.

per Mausklick meilenweit entfernt sind. Und es ist nicht sicher, ob wir dies jemals erreichen werden. Dazu sind viel zu viele an unverschlüsselten Informationen interessiert.

Der Staat will bei Verschlüsselung mitlesen können

> »[Der ehemalige englische] Premierminister David Cameron will gar keine verschlüsselte Kommunikation zulassen: ›Wollen wir in unserem Land Kommunikationsmöglichkeiten erlauben, die wir nicht lesen können? Ich sage nein, wollen wir nicht, und wir müssen dementsprechende Gesetze erlassen‹.«[7]

> »Auch [der ehemalige deutsche] Innenminister Thomas de Maizière will, dass der Staat entschlüsseln kann: ›Unsere Sicherheitsbehörden sollen, natürlich unter rechtsstaatlichen Voraussetzungen, befugt und in der Lage sein, verschlüsselte Kommunikation zu entschlüsseln, wenn dies für ihre Arbeit und zum Schutz der Bevölkerung notwendig ist‹.«[8]

> »Michael Rogers [ehemaliger NSA-Chef] will keine Hinter-, sondern eine Vordertür in Krypto-Algorithmen: ›Ich würde das nicht Hintertür nennen. Wenn ich den Ausdruck Hintertür, höre, denke ich, das klingt irgendwie dubios. Warum würden wir die Hintertür nehmen? Wir würden das ganz öffentlich machen‹.«[9]

Diese drei Aussagen mögen stellvertretend sein für die Forderung nach dem Zugriff auf verschlüsselte Informationen, wie sie immer wieder von Politikern erhoben wird.

7 Rieger 2015.

8 Ebd.

9 Ebd.

Die Botschaft ist klar: Der Staat will bei verschlüsselter Kommunikation mitlesen können. Begründet wird dies damit, dass nur so eine Verfolgung von Terroristen und Kriminellen möglich sei, die natürlich ebenfalls verschlüsselt kommunizieren.

Diese Forderung ist nachvollziehbar. Wenn eine richterliche Genehmigung vorliegt, ist gegen ein Mitlesen der verschlüsselten Informationen nichts einzuwenden. Das Problem ist nur, dass man dazu z.B. einen Zweitschlüssel oder eine Hintertür benötigt. Und wenn der Staat über einen solchen außerordentlichen Zugang verfügt, ist leider zu befürchten, dass über kurz oder lang auch Kriminelle, Terroristen sowie feindliche Staaten darüber verfügen werden. Das kann die Sicherheit der gesamten Internetinfrastruktur gefährden. Der Schaden, der dadurch entsteht, ist nach Ansicht von Experten bei weitem schlimmer als die fehlende Entschlüsselungsmöglichkeit der Informationen von Kriminellen und Terroristen.[10]

Dieses Dilemma ist schwer zu lösen. Interessanterweise legen die Enthüllungen u.a. von Snowden nahe, dass die Überwachung sich nicht nur gegen Terroristen und Kriminelle richtete, sondern u.a. auch dem Ziel der Wirtschaftsspionage diente.[11]

Zwei ganz wichtige Stellungnahmen zu diesem Thema – eine pro und eine contra Verschlüsselung durch die USA – werden daher hier aufgeführt.

Nachstehender Aufruf wurde am 28. Juli 2015 in der Washington Post veröffentlicht.

> »Warum die Angst vor der allgegenwärtigen Datenverschlüsselung übertrieben ist. […] Heutzutage bietet die allgegenwärtige Verschlüsselung wesentliche Sicherheit, da fast jeder ein vernetztes Gerät besitzt. Wenn Strafverfolgungs- und

10 Vgl. Abelson et al. 2015.

11 Vgl. Meister 2015.

> Geheimdienstorganisationen eine Zukunft ohne gesicherten Zugang zu verschlüsselter Kommunikation vor sich haben, werden sie Technologien und Techniken entwickeln, um ihre legitimen Missionsziele zu erreichen.«[12]

Die Autoren dieses Aufrufes sind Mike McConnell, ehemaliger Direktor der NSA und Direktor der Nationalen Nachrichtendienste, Michael Chertoff, ehemaliger US-amerikanischer Minister für Innere Sicherheit und Vorstandsvorsitzender der Chertoff Group, einer Beratungsfirma für Sicherheit und Risikomanagement und William Lynn, ehemaliger stellvertretender Verteidigungsminister und Geschäftsführer von Finmeccanica North America und DRS Technologies, einem Luft- und Raumfahrt- so wie Rüstungs-Unternehmen.

Sie unterstreichen in ihrem Aufruf, wie wichtig eine Ende-zu-Ende-Verschlüsselung in der heutigen Zeit ist. Das ist eine Verschlüsselung, bei der nur der Sender und der Empfänger Zugriff auf die verschlüsselte Nachricht haben. Ihrer Ansicht nach bedeutet jeder Eingriff des Staates in Verschlüsselungsmechanismen eine Schwächung des Schutzes von Informationen vor unbefugtem Zugriff. Für die Unterzeichner stellt die Sicherheit einer Kommunikationsinfrastruktur durch eine Ende-zu-Ende-Verschlüsselung ein höheres Gut als der Einbau staatlicher Überwachungsmöglichkeiten dar. Denn durch eine solche Ende-zu-Ende-Verschlüsselung ist eine Massenüberwachung aller Bürger nicht mehr möglich.

Gleichzeitig machen die Unterzeichner klar, dass ihrer Meinung nach der Staat Mittel und Wege finden wird, seine Ziele auch unter diesen Gegebenheiten zu erreichen.

---

12 »Why the fear over ubiquitous data encryption is overblown. […] Today, with almost everyone carrying a networked device on his or her person, ubiquitous encryption provides essential security. If law enforcement and intelligence organizations face a future without assured access to encrypted communications, they will develop technologies and techniques to meet their legitimate mission goals.« McConnell/Chertoff/Lynn 2015.

Das Aufregende an diesem Aufruf ist, dass er nicht von irgendwelchen Bürgerrechtsbewegungen kommt, von denen man solche Statements kennt, sondern von ehemaligen hohen Regierungsvertretern. Er kommt somit aus genau den Kreisen, die derzeit massiv eine Einschränkung der Verschlüsselung fordern, damit der Staat darauf zugreifen kann.

Nachstehender Aufruf erschien am 11. August 2015 in der New York Times. Es ist sozusagen die Gegenposition zu dem vorherigen Aufruf.

> »Wenn die mobile Verschlüsselung die Gerechtigkeit aussperrt. […] Die neuen Verschlüsselungsrichtlinien von Apple und Google haben es schwieriger gemacht, Menschen vor Kriminalität zu schützen. Wir unterstützen die Datenschutzrechte von Einzelpersonen. In Ermangelung einer Zusammenarbeit von Apple und Google müssen Regulierungsbehörden und Gesetzgeber in unseren Ländern nun ein angemessenes Gleichgewicht zwischen den geringfügigen Vorteilen der Vollplattenverschlüsselung und der Notwendigkeit lokaler Strafverfolgungsbehörden zur Aufklärung und Verfolgung von Straftaten finden. Die Sicherheit unserer Gesellschaft hängt davon ab.«[13]

Bei den Unterzeichnern handelt es sich um Cyrus Vance, Staatsanwalt des Regierungsbezirks Manhattan, François Molins, leitender Pariser Staatsanwalt, Adrian Leppard, Londoner Polizeichef, und Javier Zaragoza, leitender Staatsanwalt des Obersten Gerichtshofs in Spanien.

13 »When Phone Encryption Blocks Justice. […] The new encryption policies of Apple and Google have made it harder to protect people from crime. We support the privacy rights of individuals. But in the absence of cooperation from Apple and Google, regulators and lawmakers in our nations must now find an appropriate balance between the marginal benefits of full-disk encryption and the need for local law enforcement to solve and prosecute crimes. The safety of our communities depends on it.« Vance Jr./Molins/Leppard/Zaragoza 2015.

Sie wenden sich gegen die Verschlüsselung der gesamten Festplatte, die Google und Apple inzwischen anbieten. Ein Zugriff der Justiz ist hier nicht mehr möglich, da Apple und Google nicht im Besitz der Schlüssel sind. Die Unterzeichner führen einen Fall an, wo der Mörder nicht gefasst werden konnte, da kein Zugriff auf die verschlüsselten Inhalte von Smartphones möglich war. Sie weisen darauf hin, dass dies kein Einzelfall war, sondern immer öfter vorkommt. Im Gegenzug dazu zitieren sie den Angriff auf Charlie Hebdo, bei dem die Daten der Smartphones entscheidend für die rasche Untersuchung dieser Terroranschläge waren. Sie fordern legale Wege, um die Verschlüsselung auf modernen Smartphones umgehen zu können.

Erwähnenswert ist in diesem Zusammenhang der Vorstoß von Susan Landau, Professorin für Politik der Cybersicherheit (*cybersecurity policy*) am Worcester Polytechnic Institute (Massachusetts). Sie plädiert dafür, dass der Staat Kapazitäten ausbauen sollte, um verschlüsselte Informationen gesetzeskonform entschlüsseln zu können. Dass eine solche Vorgehensweise durchaus erfolgversprechend sein kann, zeigt das Beispiel des Attentäters von San Bernardino. Nachdem Apple sich geweigert hatte, das FBI bei der Entschlüsselung des iPhones des Attentäters zu unterstützen, beauftragte das FBI einen professionellen Hacker, dem Vernehmen nach handelt es sich um die israelische Firma Cellebrite.[14] Diese entdeckte, so wird berichtet, einen Software-Fehler im iPhone, der letztendlich das Knacken des Handy-Zugangscodes ermöglichte, ohne dabei Daten zu verlieren. Das FBI soll dafür 1,3 Millionen Dollar bezahlt haben.[15]

Wie die New York Times vor kurzem berichtete, haben mindestens 2000 Strafverfolgungsbehörden in den USA Werkzeuge, mit denen sie sich Zugriff auf verschlüsselte Smartphones verschaffen können. Eine

14 Vgl. Israelische Firma hilft FBI angeblich beim iPhone-Hack, 2016.

15 Vgl. Eisner 2016.

solche Vorgehensweise entspricht genau dem, was Susan Landau vorgeschlagen hat.[16]

Solange es Verschlüsselung geben wird, solange werden auch die Versuche, diese auszuhebeln nicht aufhören. Derzeit besonders unter Beschuss steht die Ende-zu-Ende-Verschlüsselung, bei der nur Sender und Empfänger die Nachricht lesen können. Der Anbieter kennt die Schlüssel nicht, kann somit die Nachrichten auch nicht entschlüsseln. Ginge es nach dem Willen der Strafverfolgungsbehörden, sollten Firmen wie Apple, Facebook u.a. gezwungen werden, Verschlüsselung nur dann anzubieten, wenn sie für all diese Kommunikationen auch Nachschlüssel anfertigen, die sie den Strafverfolgern bei Bedarf aushändigen können. Entsprechende Vorschläge gibt es in den USA und auch von Seiten der Europäischen Kommission.[17] Die Umsetzung dieser Vorschläge käme einer Abschaffung der Ende-zu-Ende-Verschlüsselung gleich.

Die Forderung nach Zugang zu verschlüsselten Informationen ist eine unendliche Geschichte. Gerade erst haben Regierungsvertreter aus Amerika, Kanada, Großbritannien, Australien und Neuseeland ein Kommuniqué herausgegeben, in dem sie fordern, dass die Industrie ihnen für die Strafverfolgung den Zugriff auf verschlüsselte Inhalte ermöglicht. Indien und Japan haben sich dem Aufruf angeschlossen.[18]

Ein interessantes Beispiel, was passiert, wenn der Staat selber Verschlüsselungsdienste anbietet, ist die sogenannte deutsche De-Mail.

> »Keine Regierung ist so blöd, ihren Bürgern ein abhörsicheres Kommunikationsmedium zu geben.« (Linus Neumann)[19]

16 Vgl. Nicas 2020.

17 Vgl. Moechel 2020.

18 Vgl. »Five Eyes« fordern Zugang zu verschlüsselten Apps, 2020; International Statement: End-To-End Encryption and Public Safety, 2020.

19 Totschkas_blog 2.0, 2013.

Dies ist der sehr drastische Kommentar von Linus Neumann, Sprecher des Chaos Computer Clubs Deutschland, zur so hochgepriesenen deutschen De-Mail. Über diesen Dienst können Nutzer Nachrichten und Dokumente sicher, vertraulich und nachweisbar über das Internet austauschen.

Tatsächlich ist die De-Mail ein gutes Beispiel, wie der Staat sich Zugriff auf verschlüsselte Kommunikation verschafft.

Die De-Mail wird vom Dienstanbieter, nicht vom Kunden verschlüsselt. Sie wird zum Zweck der Überprüfung auf Schadsoftware und zum Zweck der Weiterleitung an den Adressaten vom akkreditierten Dienstanbieter kurzzeitig automatisiert entschlüsselt. Über diesen Dienstanbieter kann der Staat im Bedarfsfall auf die De-Mail zugreifen. Wirklich sicher wäre eine Ende-zu-Ende-Verschlüsselung gewesen, bei der die Nachrichten auf dem Rechner des Absenders so verschlüsselt werden, dass sie erst wieder vom Empfänger auf dessen Rechner entschlüsselt werden können. Damit haben weder Provider noch Nachrichtendienste Zugriff auf den Inhalt dieser Mails. Dies war bei der De-Mail bisher nicht vorgesehen. Nach massiver Kritik an dem Konzept der De-Mail, insbesondere vom Chaos Computer Club, wird eine derartige Option tatsächlich angeboten.[20] Es ist jedoch zu befürchten, dass ein großer Teil der Nutzer der De-Mail diese zusätzliche Option nicht nutzen wird, da sie mit einem zusätzlichen Aufwand verbunden ist.

20 Vgl. Bleich 2015.