Positionspapier

Starke Verschlüsselung für mehr Sicherheit
Cyber-Sicherheit und Wirtschaftsschutz mit Verschlüsselung
Strafverfolgung und Gefahrenabwehr trotz Verschlüsselung

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Sebastian Artz
Referent IT-Sicherheit
s.artz@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Vorbemerkung

In der öffentlichen Wahrnehmung und auch im politischen Diskurs scheint ein Interessenskonflikt zwischen den Themen IT-Sicherheit und Öffentliche Sicherheit zu bestehen. Anknüpfend an die *↗ Grundsatzerklärung des Bitkom zur Verschlüsselung* werden nachfolgend verschiedene Aspekte näher beleuchtet, um diesen vermeintlichen Zielkonflikt aufzulösen.

IT-Sicherheit im Spannungsfeld von Strafverfolgung und sicherer Kommunikation

Fakt ist, Verschlüsselung ist die Basis zur Schaffung von Vertraulichkeit, die wiederum als zwingende Notwendigkeit verstanden werden muss, um Privatsphäre, freie Meinungsbildung sowie den Schutz von Unternehmensgeheimnissen überhaupt erst zu ermöglich. Um den unberechtigten Abfluss und die Veränderung sensibler Daten zu verhindern, werden unterschiedliche Verschlüsselungsprotokolle und -standards erfolgreich eingesetzt. Dabei ist Verschlüsselung atomar und binär, sie funktioniert oder sie funktioniert nicht – Zwischenzustände gibt es nicht. Unmittelbar daran anknüpfend stellt sich die Frage der korrekten Implementierung von Verschlüsselung. Die aktuellen sicheren Standards haben - soweit bekannt - keine Hintertüren, sodass niemand die Verschlüsselung grundsätzlich umgehen kann. Dies ist essenziell und unabdingbar, denn ohne die grundlegende Verlässlichkeit und Robustheit der durch Hard- und Software implementierten Verschlüsselung kann niemand Vertrauenswürdigkeit eigenständig feststellen. In der Folge würde das Vertrauen verloren gehen – und damit die Grundlage dafür, Digitalisierung als Chance zu begreifen.

Dabei muss im selben Atemzug das Thema Schwachstellen (Vulnerabilities) adressiert werden, denn jede ungeschlossene Schwachstelle unterminiert das Grundvertrauen der Anwender. Spätestens seit der »WannaCry« Attacke ist gemeinhin bekannt, wie schnell ein intransparenter Umgang mit staatlich gehaltenen Sicherheitslücken zum Risiko für alle werden kann. Hier wurden von den Diensten entdeckte aber geheim gehaltene Sicherheitslücken entwendet, um sie für eine weltweit angelegte Cyber-

Erpressungs-Attacke auszunutzen. Bei zeitiger Kenntnis der Lücken hätten die Hersteller diese schon viel früher durch Updates schließen können und so den Schaden verhindern oder begrenzen können. Daher darf eine solche absichtliche staatliche Schwächung von IT-Sicherheitsprodukten auch in Zukunft nicht erlaubt sein. Durch staatliche Maßnahmen dürfen auch Hersteller nicht gezwungen werden Hintertüren einzubauen, weil diese automatisch zu einer Sollbruchstelle in der IT-Sicherheit führen. Hersteller könnten nicht sicherstellen, dass diese nicht allgemein bekannt wird. Sicherheitslücken, wie die hinter der »WannaCry« Attacke, werden gehandelt und besitzen schon jetzt einen hohen Schwarzmarktwert. Hersteller könnten nicht verhindern, dass sämtliche Produkte genau über diese absichtliche Schwachstelle gleichzeitig angegriffen würden. Backdoors haben das Potenzial, hier buchstäblich die Büchse der Pandora zu öffnen. Ein Verbot von Backdoors ist jedoch nur dann sinnvoll, wenn auch der Ankauf oder das Teilen von Schwachstellen gesetzlich untersagt wird und auch die staatlichen Akteure einer Meldepflicht für die entdeckten Schwachstellen unterliegen.

In diesem Kontext lohnt der Blick auf eine Aussage des Präsidenten des BSI aus dem November 2020: »Digitale Produkte mit Schwachstellen im Zweifel nicht zuzulassen oder zu zertifizieren, gehört fürs BSI zur nationalen digitalen Souveränität.« Als Bitkom teilen wir diese Auffassung und die Wirtschaft sieht sich dabei auch selbst in der Pflicht, Schwachstellen konsequent zu schließen. Die Bundesregierung ist aufgerufen, sich hier auch für eine zwischenstaatliche Lösung einzusetzen, da IT-Sicherheit nicht an Landesgrenzen endet. Eine verantwortungsvolle, international anerkannte und gelebte Regelung ist notwendig, um Schwachstellen nicht öffentlich werden zu lassen, sondern es den Herstellern zu ermöglichen, rasch Sicherheitsupdates zu liefern.

Für die wissensgetriebene Wirtschaft ist es überlebenswichtig, sichere Verschlüsselung anzuwenden und verlässlich zu nutzen. Gerade die hochinnovative und international-orientierte deutsche Wirtschaft muss sich auf den Schutz ihrer Geschäftsgeheimnisse durch sichere kryptografische Methoden verlassen können. Die Bundesregierung muss sich weiterhin für sichere Unternehmenskommunikation international tätiger Konzerne einsetzen.[1] Darüber hinaus darf Europas Vorbildfunktion beim Schutz personenbezogener Daten durch die Datenschutzgrundverordnung und die aufgebaute Reputation in Bezug auf sichere Technologien nicht konterkariert werden. Der negative Effekt auf den Wirtschaftsstandort ist kaum zu überschätzen. Europa darf seine Vorbild-

[1] Retrospektiv sollte bspw. nicht vergessen werden, dass es, seinerzeit und in Anbetracht der ausufernden chinesischen Cyber-Sicherheitsgesetzgebung, die VPN-Verschlüsselung sogar auf die Agenda der Regierungskonsultation mit China geschafft hat. Die VPN-Verschlüsselung ist zwar nicht grundsätzlich verboten worden, wird aber als genehmigungspflichtig erachtet. Deutschland und Europa sollte hier gemäß der europäischen Werte andere Wege gehen.

rolle und starke Position hier nicht aufgeben – auch weil zu erwarten ist, dass sonst ein Dominoeffekt eintritt und weitere Rechtsräume dem »Beispiel« folgen würden.

Jedoch müssen auch Sicherheitsbehörden in der Lage sein, auch in schwierigen Fällen und mit hoher digitaler Kompetenz, ihrem Strafverfolgungs- und Ermittlungsauftrag und der Schutzpflicht des Staates wirksam nachzukommen. Auf der anderen Seite verschlüsseln auch Straftäter und Terroristen zunehmend ihre Kommunikation und erschweren die Arbeit der Strafverfolgungsbehörden.[2] Somit stellt sich die folgende Frage: **IT-Sicherheit oder Strafverfolgung? Die Antwort lautet: Beides!**

Eindeutiger Rechtsrahmen

Wir brauchen einen eindeutigen Rechtsrahmen als Brücke zwischen diesem vermeintlichen Spannungsfeld. In engen Grenzen und unter richterlichem Vorbehalt muss eine Kooperation von Unternehmen und Sicherheitsbehörden, zwischen Wirtschaft und Staat ermöglicht werden, bspw. zur Abwehr erheblicher Gefahren für die Öffentlichkeit oder das Leben. Dabei kommt es insbesondere auf die Verhältnismäßigkeit der Maßnahmen an. Das Spannungsfeld bewegt sich deshalb zwischen drei wesentlichen Punkten:

1. effektive Sicherheitsbehörden
2. sichere vertrauliche Kommunikation
3. Garantie für Unternehmen an ihrem geistigen Eigentum

Diese schwierige Abwägung zwischen dem Schutz der Bevölkerung vor erheblichen Straftaten und den Grundrechten auf Datenschutz und Privatsphäre, aber auch das Grundrecht auf wirtschaftliche Entfaltung und das geistige Eigentum der Unternehmen, müssen hier berücksichtigt werden. Diese Abwägung muss gesetzlich eindeutig geregelt werden. So könnte bestimmt werden, unter welchen Voraussetzungen und in welchem Umfang Unternehmen mit den Sicherheitsbehörden im Einzelfall zur Abwehr von schweren Straftaten zusammenarbeiten dürfen. Gleichzeitig sollte es für Unternehmen transparent sein, welche Einflüsse die Ermittlungen auf ihr Produkt und ihre Infrastrukturen haben.

Nicht zu vernachlässigen ist die Tatsache, dass es um Grundsatz- und die Grundwerte betreffende Fragestellungen geht. Entsprechend behutsam sollten entsprechende Abwägungen stattfinden und grundrechtsschonende Strafverfolgungsmethoden im digitalen Raum Vorrang haben. Die Rechte der Betroffenen müssten durch richterliche

[2] Der bereits zitierte Präsident des BSI sagte bereits im Jahr 2014: »die Organisierte Kriminalität verdient seit 2009 im Bereich Cyber mehr Geld als mit Drogen«.

Kontrolle und G10-Kommission[3] gewahrt bleiben. Es bedarf eines normativen rechtsstaatlichen Korrektivs. Während sich die Enquete-Kommission Künstliche Intelligenz mit den Auswirkungen des zunehmenden Einsatzes Künstlicher Intelligenz beschäftigt können wir nicht im gleichen Atemzug darüber sprechen, Verschlüsselung möglichst unwirksam zu gestalten. Andernfalls entziehen wir den Potenzialen der Digitalisierung den Boden unter den Füßen.

Als Bitkom sind wir bereit, diese bewusste Abwägung aktiv und konstruktiv mitzugestalten, denn letztlich kommt es auch darauf an, Terrorismus, organisierte Kriminalität, Spionage, Sabotage kritischer Infrastrukturen und ähnliche Straftaten zu verhindern und effizient zu verfolgen. Dies ist Aufgabe der Sicherheitsbehörden und auch die Erwartung der Bürger und Unternehmen.

Vertrauen, Kontrolle und Transparenz bei staatlichen Stellen ausbauen

Die Sicherheitsbehörden müssen so ausgestattet sein, dass sie ihren jeweiligen Aufträgen bestmöglich im Rahmen von Recht und Gesetz nachkommen können. Diese klar umrissenen Aufträge müssen jedoch transparent sein und ihre rechtmäßige Erfüllung muss kontrolliert werden können. Nur mit wirksamen Kontrollmechanismen unter Berücksichtigung der Gewaltenteilung können das Vertrauen der Bürger und der Unternehmen erhalten werden. Hierzu gehört auch, dass die Sicherheitsbehörden technisch, personell und organisatorisch in der Lage sein müssen, Sicherheit zu gewährleisten.

All das ist unweigerlich mit Kosten verbunden. In Anbetracht der die IT-Sicherheit unterminierenden Optionen und der damit einhergehenden Opportunitätskosten sollten wir diese Ausgaben aber nicht scheuen. Starke Verschlüsselung unter Kosten- und Aufwands-Gesichtspunkten wegzurationalisieren darf keine Option sein. Neben die bessere und zeitgemäße technische Ausstattung von Polizei und Behörden tritt mehr gut ausgebildetes Ermittlungspersonal im digitalen Raum, das in der Breite gut gestärkt wird durch präventiv-wirkende Sozialarbeit. Rückgrat dieser starken Sicherheitsarchitektur ist die vertrauensvolle und effiziente Vernetzung aller Sicherheitsbehörden, Bund- und Länder-übergreifend, europäisch und international.

[3] Die G 10-Kommission entscheidet von Amts wegen als unabhängiges und an keine Weisungen gebundenes Organ über die Notwendigkeit und Zulässigkeit sämtlicher durch die Nachrichtendienste des Bundes (Bundesnachrichtendienst, Bundesamt für Verfassungsschutz, Militärischer Abschirmdienst) durchgeführten Beschränkungsmaßnahmen im Bereich des Brief-, Post- und Fernmeldegeheimnisses nach Artikel 10 des Grundgesetzes (GG).

»Lawful Interception« ist nicht zuletzt deshalb ein anerkanntes Mittel, weil es klar begrenzt und für alle beteiligten Parteien an hohe Hürden geknüpft ist. Dies ist beim Wunsch nach Front- oder Backdoors nicht der Fall. Der Blick muss also in Richtung des standardisierten Schnittstellenmanagements gehen. Entsprechende Schnittstellen werden fortlaufend erweitert, wie zuletzt auch für Messaging Dienste.[4] Der Staat ist aufgerufen, sich neben den bereits eingebundenen Netzbetreibern und Systemlieferanten noch aktiver in den Standardisierungsgremien einzubringen, um benötigte sichere Schnittstellen-Definitionen mitzugestalten. Bitkom vertritt die Auffassung, dass eine berechtigte, richterlich angeordnete, anlassbezogene und eng begrenzte Strafverfolgung im digitalen Raum möglich sein muss (und auch im Grunde ist).

Um die gesellschaftliche Legitimation für die Art der Zusammenarbeit von Sicherheitsbehörden untereinander, aber auch mit Unternehmen sicherzustellen, ist Transparenz über Arbeitsweisen und Prozesse zwischen den Akteuren erforderlich. Transparenz über die zulässigen Vorgehensweisen schützt gleichzeitig die Unternehmen vor einem Vertrauensverlust. Transparenzberichte, wie sie Provider und Netzbetreiber zu Überwachungsanordnungen der Telekommunikation regelmäßig veröffentlichen, können dieses Ziel seitens der Wirtschaft ergänzen. Sicherheitsinteressen dürfen durch diese Transparenz natürlich nicht berührt werden und es muss, wo nötig, auch Geheimhaltung gewährleistet sein. In einer globalisierten und digitalisierten Gesellschaft gilt jedoch auch, dass Herausforderungen nicht mehr nur allein und national gelöst werden können, sondern Informationen verantwortungsvoll geteilt werden müssen. Ein Beispiel für internationale Zusammenarbeit könnte das gemeinsame Finden von Ermittlungsansätzen im jeweiligen Einzelfall mit Hilfe der Wirtschaft sein.

Stärkung der Kompetenzen der Nutzer und Fortführung des gesellschaftlichen Diskurses

Zur Sicherheit in der Digitalisierung gehört auch die stete Stärkung der Kompetenz der Nutzer. Sie müssen Risiken kompetent einschätzen und sich verantwortungsvoll verhalten können. Fahrlässigkeit beim Umgang mit Sicherheitsupdates oder schwache Passwörter, die vorgesehene Sicherheitsmechanismen aushebeln können, darf nicht länger akzeptabel sein. Denn Hersteller, die Schwachstellen melden und Updates bereitstellen, stehen auf verlorener Front, wenn Anwender keine Updates installieren oder ihre Systeme ungepatcht lassen. Daher muss weitere Sensibilisierung und Aufklärung als staatliche Daueraufgabe im Zusammenspiel mit den Initiativen der Wirtschaft etabliert werden. Automatische Updates können den Konsumenten zudem dabei helfen, sicherheitsrelevante Updates einzuspielen. Bei sicherheitskritischen Produkten könnte die

[4] ETSI TS 103 707 v1.1.1 (2020-03)

weitere Nutzbarkeit ohne ein entsprechendes Update eingeschränkt werden. Die transparente Kommunikation von zu erwartenden Updatezyklen kann ein Mosaikstein im Gesamtkontext sein. Auch ein freiwilliges, aussagekräftiges und idealerweise europäisches IT-Sicherheitskennzeichen ist ein Hebel, dem wir als Digitalwirtschaft grundsätzlich positiv gegenüberstehen, um das Nutzerverhalten zu stärken.

Bitkom hält einen breiten und dauerhaften gesellschaftlichen Diskurs zu dem hier skizzierten Spannungsfeld für unerlässlich. Das BSI hat in der jüngsten Zeit auch die Verantwortung für die Sicherheit der Gesellschaft wieder verstärkt in den Mittelpunkt gerückt. Mit dem IT-Sicherheitsgesetz 2.0 bekommt das BSI zusätzliche neue Kompetenzen im Bereich des digitalen Verbraucherschutzes. Gemeinsam mit Netzpolitikern, zivilgesellschaftlichen Initiativen und mit Einbindung der Wissenschaft halten wir es für sinnvoll, einen institutionell verankerten Rahmen für einen dauerhaften Diskurs zu schaffen. Ähnlich wie bei den Fragen zu selbstfahrenden Fahrzeugen kann sich die Gesellschaft mit Politik und Verwaltung einen gemeinsamen Kurs geben. Eine zeitgemäße Lösung für mehr Sicherheit in der gesamten Gesellschaft muss dann allerdings auch auf europäischer Ebene vorangetrieben werden.

Informationstechnik ist bereits heute in vielen Bereichen die Grundlage für ein funktionierendes Gemeinwesen und wirtschaftliche Wertschöpfung. Dessen und der damit einhergehenden Verantwortung ist sich die durch Bitkom vertretene Branche bewusst und nimmt diese aktiv an. Deshalb entwickeln wir sichere Produkte, setzen sicheren Informationsaustausch/Datentransfer um und reagieren bei festgestellten Sicherheitslücken schnell. Ausdruck dieser wahrgenommenen Verantwortung ist aber auch, dass wir uns der drohenden flächendeckenden Schwächung etablierter Sicherheitsmechanismen entgegenstellen.

Bitkom vertritt mehr als 2.700 Unternehmen der digitalen Wirtschaft, davon gut 2.000 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.