Positionspapier

Cyber-Sicherheit und Wirtschaftsschutz mit Verschlüsselung
Strafverfolgung und Gefahrenabwehr trotz Verschlüsselung

AK Wirtschaftsschutz / AK Sicherheitspolitik / AK Öffentliche Sicherheit

22.09.2017

Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Marc Bachmann
Bereichsleiter Luftfahrt & Verteidigung
T +49 30 27576-102
m.bachmann@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Bitkom vertritt mehr als 2.500 Unternehmen der digitalen Wirtschaft, davon gut 1.700 Direktmitglieder. Sie erzielen mit 700.000 Beschäftigten jährlich Inlandsumsätze von 140 Milliarden Euro und stehen für Exporte von weiteren 50 Milliarden Euro. Zu den Mitgliedern zählen 1.000 Mittelständler, 400 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Hardware oder Consumer Electronics her, sind im Bereich der digitalen Medien oder der Netzwirtschaft tätig oder in anderer Weise Teil der digitalen Wirtschaft. 78 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, 9 Prozent kommen aus Europa, 9 Prozent aus den USA und 4 Prozent aus anderen Regionen. Bitkom setzt sich insbesondere für eine innovative Wirtschaftspolitik, eine Modernisierung des Bildungssystems und eine zukunftsorientierte Netzpolitik ein.

Zusammenfassung

Die Digitalisierung bietet enorme Vorteile und stellt uns vor neue gesellschaftliche Herausforderungen. Eine ist die aktuelle Diskussion um das Dilemma von Software-Hintertüren (Backdoors – siehe Kasten Seite 2). Bitkom richtet hierfür folgende Handlungsempfehlungen an die Politik.

- **Es braucht ein klares Verbot, IT staatlicherseits absichtlich zu schwächen.**
- **Auch eine Meldepflicht für staatliche Akteure für entdeckte Sicherheitslücken ist notwendig.**
- **Die Zusammenarbeit von Wirtschaft und Sicherheitsbehörden braucht einen eindeutigen Rechtsrahmen.**
- **Vertrauen durch Kontrolle und Transparenz stärken: Die Sicherheitsbehörden brauchen mehr Ausstattung - nicht mehr Befugnisse.**
- **Die Sicherheitskompetenz der Nutzer muss nachhaltig gestärkt werden und ein breiter gesellschaftlicher Diskurs muss etabliert werden.**

IT-Sicherheit im Spannungsfeld von Strafverfolgung und sicherer Kommunikation für Bürger und Wirtschaft

Vorbemerkung

In der öffentlichen Wahrnehmung und auch im politischen Diskurs scheint ein Interessenskonflikt zwischen den Themen IT-Sicherheit und Öffentliche Sicherheit zu bestehen. Hintergrund ist zum einen die Notwendigkeit der sicheren Kommunikation als Teil der IT-Sicherheit: Regierungskommunikation, Unternehmensgeheimnisse oder der Schutz der Privatsphäre sind Werte, die auf Vertraulichkeit angewiesen sind und die gut geschützt werden müssen. Auf der anderen Seite verschlüsseln auch Straftäter und Terroristen zunehmend ihre Kommunikation und erschweren die Arbeit der Strafverfolgungsbehörden.

Die „WannaCry“ Attacke im Mai 2017 hat gezeigt, wie schnell ein heimlicher 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.

Bundesinnenminister Thomas De Maizière fordert die gesetzliche Gleichstellung bei der Überwachung von SMS und Messenger Diensten, erklärt aber nicht, wie dieses Dilemma sinnvoll aufgelöst werden soll.

Bitkom fordert daher gemeinsam mit Industrie und Strafverfolgungsbehörden eine sinnvolle Lösung finden. Nicht durch Geheimhaltung sondern durch offenen gesellschaftlichen Diskurs sollen berechtigte Sicherheitsinteressen ausgeglichen werden. Bitkom möchte hier einen Beitrag leisten und über inhaltliche Vorschläge eine Brücke zu bauen. Folgende Aspekte halten wir dabei für wesentlich:

IT-Sicherheit oder Strafverfolgung: Beides!

Für die Wirtschaft aber auch für Bürger ist es essentiell sichere Verschlüsselung anzuwenden und zu nutzen. 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. IT-Sicherheit und Beides sind zentrale Elemente der Sicherheit.

Backdoors: Gemeint sind im Code der Software versteckte Zugänge zu verschlüsselter Kommunikation oder die Hinterlegung von sog. Generalschlüsseln bei staatlichen Akteuren, die dann jederzeit den Zugang zur verschlüsselten Kommunikation hätten. Übersehen wird hier, dass technisch jeder die Hintertür finden und nutzen kann und ein digitaler Generalschlüssel unendlich vervielfältigt und weitergegeben werden kann.

Ein Aspekt hierbei ist die sichere Verschlüsselung. Um den unberechtigten Abfluss und die Veränderung sensibler Daten zu verhindern, werden unterschiedliche Verschlüsselungsprotokolle und -standards erfolgreich eingesetzt. Die aktuellen sicheren Standards haben - soweit bekannt - keine Hintertüren, so dass niemand die Verschlüsselung grundsätzlich umgehen kann. Trotzdem setzen verschiedene Staaten auf verschiedenen Krypto-Algorithmen. So präferiert das BSI beispielsweise den Einsatz von Brainpool-Kurven.

Seit einiger Zeit fordern Sicherheitsbehörden die Implementierung von Hintertüren (Backdoors) oder Masterschlüsseln in die sicheren Verschlüsselungsstandards, um Strafverfolgungsbehörden im Bedarfsfall zu ermöglichen die Kommunikation zwischen Kriminellen oder Terroristen mitzulesen. Hierdurch wird jedoch nicht mehr Sicherheit geschaffen, sondern im Gegenteil IT-Sicherheit dauerhaft geschwächt. Es wird die Tatsache übergangen, dass genau diese Hintertüren dann auch von Kriminellen ausgenutzt werden könnten. Jeder Nachrichtendienst, Cyber-Kriminelle, Hacker und unlauterer Wettbewerber wird nach einer Hintertür suchen, wenn davon auszugehen ist, dass es sie gibt. Es ist dann nur eine Frage der Zeit (wahrscheinlich von Wochen) dass sie gefunden wird.

Klares Verbot von Software-Hintertüren (Backdoor-Verbot)

Daher darf eine solche absichtliche staatliche Schwächung von IT-Sicherheitsprodukten 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. Dieser würde weiter gesteigert, wenn alle Produkte eine Zwangs-Lücke hätten. Hersteller könnten nicht verhindern, dass sämtliche Produkte genau über diese absichtliche Schwachstelle gleichzeitig angegriffen würden. Backdoors öffnen buchstäblich die Büchse der Pandora.

Die Entwicklung sicherer Produkte ist entscheidend für die Gewährleistung der Sicherheit einer vernetzten Gesellschaft.

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. 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 selbst nicht öffentlich werden zu lassen, sondern es den Herstellern zu ermöglichen, rasch Sicherheitsupdates zu liefern.

Eindeutiger Rechtsrahmen

Wir brauchen einen eindeutigen Rechtsrahmen als Brücke zwischen diesem 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

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)

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 der sicheren Lösungen.

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 haben. Die Rechte der Betroffenen müssten durch richterliche Kontrolle oder eine Art G10-Kommission gewahrt bleiben. Letztlich kommt es darauf an, Terrorismus, organisierte Kriminalität, Spionage, Sabotage kritischer Infrastrukturen und ähnliche Straftaten zu verhindern und effizient zu verfolgen. Dies ist das legitime Ziel sämtlicher Sicherheitsbehörden und auch die Erwartung der Bürger und Unternehmen.

1. Nach Abschaltung der ISDN Telefonie Ende 2018 muss die Telekommunikationsüberwachung gänzlich den Datenverkehr erfassen, worauf sich die Sicherheitsbehörden einstellen müssen.

2. Bei einer regulären Beschlagnahmung (außerhalb von Cybercrime) fallen heutzutage schon leicht 6000 Gigabyte auf Datenträgern in einem einzigen Haushalt an, deren Analyse Wochen dauern kann.

Vertrauen und Kontrolle bei staatlichen Stellen ausbauen

Die Sicherheitsbehörden müssen so ausgestattet sein, dass sie ihren jeweiligen Aufträgen bestmöglich und effizient 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.

Hierzu gehört auch, dass die Sicherheitsbehörden technisch, personell und organisatorisch in der Lage sein müssen, Sicherheit zu gewährleisten (siehe Kasten). Auch sie sollten von den Vorteilen der Digitalisierung profitieren und beispielsweise frei verfügbare Big Data effizient auswerten und nutzen können, mit lernenden Algorithmen vorhersagbare Verbrechensbekämpfung leisten und in gut ausgestatteten Polizei-Cloud-Diensten sicher arbeiten und kommunizieren können. Kurz: Polizei braucht bessere und zeitgemäße Ausstattung, sowie eine sinnvolle Vernetzung aller Sicherheitsbehörden- national und international.

Durch die Standardisierung wurden Schnittstellen zum „gesetzeskonformen Abhören“ („Lawful Interception“) geschaffen. Die Ausweitung dieser Standards könnte ein Weg sein, um diese Aufgabe zur Kontrolle auch für weitere Protokolle zu ermöglichen. Hier ist der Staat aufgerufen, sich aktiv in den Standardisierungsgremien einzubringen, um benötigte Schnittstellen-Definitionen zu schaffen.

Transparenz über die Arbeitsweisen und Prozesse

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. Es ist Aufgabe des Rechtsrahmens diese Transparenz mittels formaler Vorgaben herzustellen. 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 internationalen Zusammenarbeit könnte das gemeinsame Finden von Ermittlungsansätzen im jeweiligen Einzelfall mit Hilfe der Wirtschaft oder Dritter sein, wie dies bei der Aufklärung des Hacks auf die Router im November 2016 grenzübergreifend vorbildlich funktioniert hat.

Stärkung der Nutzungskompetenz

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 akzeptable sein. Daher muss weitere Sensibilisierung und Aufklärung als staatliche Daueraufgabe im Zusammenspiel mit den Initiativen der Wirtschaft etabliert werden.

Gesellschaftlichen Diskurs fortführen

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. 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.