Grundsatzerklärung des Bitkom zur Verschlüsselung

Verschlüsselung ist unteilbar

Seit vielen Jahren fordern Sicherheitsbehörden immer wieder die Implementierung von Hintertüren (Backdoors) oder Generalschlüsseln, mit der Begründung damit die Strafverfolgung zu verbessern und so die Kommunikation zwischen Kriminellen oder Terroristen im Klartext mitlesen zu können. Mit dem Resolutionsvorstoß auf europäischer Ebene im Rahmen der deutschen Ratspräsidentschaft 2020 zum künftigen Umgang mit verschlüsselter Kommunikation erreicht die Debatte allerdings eine bislang ungekannte Intensität und Eingriffstiefe. Verschlüsselung ist der einzig mögliche Weg, vertraulich zu kommunizieren – ein unteilbares demokratisches Grundrecht. Die Diskussion über die »Schwächung« von Verschlüsselung suggeriert, dass Verschlüsselung teil- oder dosierbar sei. Das ist nicht der Fall. Aus technischer Sicht ist Verschlüsselung binär – sie ist sicher oder eben nicht. Daher sieht sich Bitkom veranlasst, seine Position erneut deutlich zu unterstreichen und sich zugleich konstruktiv in die Debatte einzubringen.

Backdoors: Gemeint sind bewusst eingerichtet Zugänge in IT-Systemen, die genutzt werden können, um verschlüsselte Kommunikation einzusehen. Sie können durch gezielte Schwachstellen realisiert werden, die den Zugriff auf unverschlüsselte Daten ermöglichen oder durch Hinterlegung von Generalschlüsseln bei staatlichen Akteuren, die dann jederzeit die Entschlüsselung der abgehörten verschlüsselten Kommunikation ermöglichen. Übersehen wird hier, dass technisch jedermann die Hintertür finden und nutzen kann und ein digitaler Generalschlüssel unendlich vervielfältigt und weitergegeben werden kann. Weitehin wird dabei vernachlässigt, dass sich Schwachstellen in Verschlüsselungsmechanismen nicht nur im Zielsystem selbst auswirken können, sondern auch in anderen Systemen, die ähnliche Verschlüsselungsmechanismen nutzen.

Backdoors sind Schwachstellen und nicht staatlich kontrollierbar

Bitkom ist der festen Überzeugung, dass die zwangsweise Einführung von Backdoors nicht zu mehr Sicherheit führt. Vielmehr wird die IT-Sicherheit dauerhaft und für alle geschwächt. Sichere (Ende-zu-Ende) Verschlüsselung ist ein Grundpfeiler des Wirtschaftsstandorts Deutschland und darf nicht durch kontraproduktive Backdoor-

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

Pflichten zerstört werden. Hintertüren lassen sich durch alle denkbaren Akteuren ausnutzten. Ihre Verwendung ist nicht auf einen rechtmäßigen Einsatz begrenzbar. Dabei gilt grundsätzlich: Technologie ist nicht gut oder schlecht, Technologie ist immer nur ein Mittel zum Zweck. Jeder Cyber-Kriminelle, Nachrichtendienst, Hacker und unlauterer Wettbewerber wird motiviert und unmittelbar belohnt, aktiv nach Hintertüren zu suchen. Es ist dann nur eine Frage der Zeit, dass Backdoors aufgespürt und nach Belieben ausgenutzt werden – egal ob zur industriellen Spionage, Sabotage kritischer Infrastrukturen oder zu Monetisierungszwecken.

Strafverfolgung braucht die richtigen Instrumente

Gleichwohl ist sich Bitkom der ordnungs- und sicherheitspolitischen Dimension bewusst und vertritt die Auffassung, dass Sicherheitsbehörden in der Lage sein müssen, auch in schwierigen Fällen und mit hoher digitaler Kompetenz, ihrem Strafverfolgungs- und Ermittlungsauftrag sowie der Schutzpflicht des Staates wirksam nachzukommen. Terrorismus, organisierte Kriminalität, Kindesmissbrauch oder Cybercrime müssen durch den Staat konsequent verfolgt werden. Die Digitalwirtschaft steht mit Wissen und Technologie bereit, um staatlichen Behörden bei ihren Aufgaben bestmöglich zu unterstützen. Sie ist dabei aber kein unmittelbarer Erfüllungsgehilfe oder eine privatwirtschaftliche Exekutionsinstanz hoheitlicher Kernaufgaben.

Bedauerlicherweise werden allzu häufig tragische Vorfälle aus dem gesellschaftspolitischen Kontext reflexartig zum Anlass genommen und nicht selten aus dem Kontext gerissen, um mehr Befugnisse für die Sicherheitsbehörden zu fordern. Dabei liegt natürlich auf der Hand, dass Erfolge der Sicherheitsbehörden häufig im Verborgenen bleiben, Misserfolge aber umso intensiver in der breiten Öffentlichkeit diskutiert werden. Argumentativ stehen dann oft fehlende Befugnisse im Fokus, statt der dringend benötigte Kompetenzaufbau und Digitalisierungsfortschritt der Sicherheitsbehörden.

Die ins Visier genommenen kriminellen Zielgruppen dürfen von niemandem unterschätzt werden. Andernfalls besteht das Risiko, einem »Straßenlampeneffekt« zu unterliegen. Wer Kriminelle nur dort sucht, wo der Generalschlüssel ins Schloss passt, übersieht, dass es sich um hochaufmerksame, agile und in kreativen Optionen denkende Personengruppen handelt. Während die Zielobjekte auf Kommunikationsmethoden und Systeme umsteigen, von denen sie wissen, dass Behörden keinen Zugang haben, bleibt der Bürger in unsicheren Systemen zurück. Verdrängungseffekte, die die Ziele der Strafverfolger zur Nutzung von Diensten und Kommunikationstechniken motivieren, die außerhalb des gesetzlich erreichbaren Radius liegen, gilt es jederzeit mitzudenken.

Güterabwägung gefordert

Das sensible Thema und die Weiterentwicklung staatlicher Eingriffsrechte braucht eine detaillierte Güterabwägung, um zu gewährleisten, dass Maßnahme, Zweck und be-

troffene Interessen in Balance bleiben. Dazu zählt auch eine konstruktive, nicht politisierte Debatte über die Möglichkeiten des Lawful Interception – anlassbezogene, richterlich angeordnete Interventionsmöglichkeiten im Bereich der Telekommunikation. Die Notwendigkeit und Rechtmäßigkeit von Lawful Interception als Instrument der Strafverfolgung unterstützt der Bitkom, allerdings ausschließlich auf Basis der Verhältnismäßigkeit für die Allgemeinheit. Zur Bewertung brauchen wir ein normatives Korrektiv, bspw. in Form eines breiten Gesellschaftskomitees.

Vor diesem Hintergrund fordert Bitkom, gemeinsam mit den Strafverfolgungsbehörden tragbare Lösungen zu finden. Nicht durch Geheimhaltung, sondern durch offenen, gesellschaftlichen Diskurs sollen berechtigte Sicherheitsinteressen Rechnung getragen werden. Bitkom möchte hier einen Beitrag leisten und über inhaltliche Vorschläge eine Brücke bauen. Dazu verweisen wir auf die

Grundsatzerklärung des Bitkom zur Verschlüsselung

- IT-Sicherheit ist nicht alles aber ohne IT-Sicherheit ist alles nichts. Es braucht ein klares Verbot, IT staatlicherseits absichtlich zu schwächen oder den Einsatz von IT-Schutzmaßnahmen einzuschränken – egal ob Back- oder Frontdoor.
- Melde- und Veröffentlichungspflicht entdeckter Sicherheitslücken – auch für staatliche Stellen.
- Vertraulichkeit der Kommunikation ist ein unteilbares Grundrecht.
- Die Entscheidungsgewalt über Verschlüsselung auf Sicherheitsbehörden zu übertragen, ist weder technisch möglich noch durchsetzbar.
- Die Zusammenarbeit von Wirtschaft und Sicherheitsbehörden braucht einen eindeutigen Rechtsrahmen. Dies gilt insbesondere für anlassbezogene, richterlich angeordnete staatliche Überwachungsmöglichkeiten und die Standardisierung potenziell nutzbarer Schnittstellen.
- Die Sicherheitsbehörden brauchen mehr und digital geschultes Personal um die existierenden Maßnahmen ausschöpfen zu können, sowie bessere technische Ressourcen. Eine Vereinfachung des Erfahrungsaustausches zwischen Industrie und Sicherheitsbehörden kann den Kompetenzaufbau der Behörden vereinfachen.
- Die Sicherheitskompetenz der Nutzer muss nachhaltig gestärkt und hierfür ein breiter gesellschaftlicher Diskurs etabliert werden.

Vor diesem Hintergrund empfiehlt Bitkom die Einrichtung eines breiten Gesellschaftskomitees »Freiheit und Sicherheit« mit dem Auftrag, die Verhältnismäßigkeit von Verschlüsselung und vertrauenswürdiger digitaler Kommunikation zu den Interessen der Strafverfolgung aus ethischer und rechtlicher Sicht zu bewerten.

Anknüpfend an die vorliegende *Grundsatzerklärung zur Verschlüsselung* verweisen wir auf unser ausführliches Bitkom Positionspapier ↗ *»Starke Verschlüsselung für mehr Sicherheit – Cyber-Sicherheit & Wirtschaftsschutz mit Verschlüsselung, Strafverfolgung & Gefahrenabwehr trotz Verschlüsselung«*.