GRUNDSÄTZE FÜR DIE VERSCHLÜSSELUNG

Umfassender Ansatz zur weltweiten Erhöhung der Internetsicherheit, öffentlichen Sicherheit, Privatsphäre & des Wohlstands

Die aktuell geführte und durchaus polarisierende Debatte über den Einsatz von Verschlüsselungstechnologien zur Erhöhung der Sicherheit geht bedauerlicherweise davon aus, dass aus allen Lösungen Gewinner und Verlierer hervorgehen. Wir weisen diese Vorstellung entschieden zurück.

Zunächst erfordert die effektive Berücksichtigung aller legitimen Interessen die Anerkennung von zwei Gegebenheiten: einerseits, dass der verstärkte Einsatz von sicheren Informationstechnologien unseren Alltag bereichert, die Wirtschaft beflügelt und zu mehr Freiheit für den Einzelnen führt. Zum anderen, dass Akteure in unrechtmäßiger Absicht Sicherheitstools nutzen, um ihre kriminellen Ziele – vom Terrorismus über Gewaltverbrechen bis Cyberattacken – zu erreichen.

Aufgrund dieser Bedingungen ergeben sich zwei Ziele, die beide umgesetzt werden müssen:

1. **Kriminellen und Terroristen muss Einhalt geboten werden.**

2. **In unserem digitalen Alltag muss die Sicherheit und Privatsphäre der Bürger gewährleistet werden.**

Eine nachhaltige Verschlüsselungslösung schafft das Gleichgewicht zwischen den berechtigten Ansprüchen, Anforderungen und Verantwortlichkeiten von:

» **Regierungen,** deren Aufgabe es ist, personenbezogene und vertrauliche Daten, die ihnen vorliegen, zu schützen sowie terroristische und kriminelle Handlungen zu verhindern und Straftäter zu verfolgen.

» **Bürgern,** die ein Recht auf die Sicherheit und den Schutz ihrer persönlichen Daten haben.

» **Anbietern von kritischen Infrastrukturen und grundlegenden Versorgungsleistungen** wie Wasser- und Stromversorgungsunternehmen, Verkehrsbetriebe, Banken und Gesundheitsanbieter, die ihre Geschäftsaktivitäten vor Cyberangriffen schützen müssen.

» **Drittunternehmern,** deren Aufgabe es ist, personenbezogene Daten und vertrauliche Geschäftsinformationen zu verwalten und die ihnen anvertrauten Daten zu sichern.

» **Innovatoren,** die Produkte und Dienste entwickeln, um unseren Alltag zu verbessern und das Wirtschaftswachstum ohne staatliche Vorgaben zu steigern.

Weiterlesen >>

GRUNDSÄTZE FÜR MASSNAHMEN

Es bedarf der gezielten Zusammenarbeit vieler Gruppen, um die Debatte um Verschlüsselungstechnologien voranzutreiben und Lösungen zu entwickeln. Wir werden alle Gesetzes-, Verordnungs- und Richtlinienvorschläge zu Verschlüsselungsthemen anhand der nachstehenden Grundsätze bewerten:

1. **Verbesserung der Datensicherheit:** Anbietern von Datendiensten, beispielsweise von Diensten für das Speichern, Verwalten oder Übermitteln von personenbezogenen Daten oder Unternehmensdaten muss gestattet sein, die jeweils beste verfügbare Technologie einzusetzen, um Angriffe auf Daten beziehungsweise Organisationen und Personen, die diese Dienste nutzen, abzuwehren.

2. **Stärkung der Strafverfolgung und Terrorismusbekämpfung:** Strafverfolgungsbehörden sollten vorbehaltlich der entsprechenden Datenschutzrechte und Grundfreiheiten die besten verfügbaren Ressourcen, Informationen und Instrumente nutzen können, um terroristische und kriminelle Handlungen zu verhindern und diese strafrechtlich zu verfolgen.

3. **Förderung des Datenschutzes:** Menschen haben ein Recht auf Sicherheit im öffentlichen, privaten und beruflichen Umfeld und bei ihren Interaktionen.

4. **Schutz von vertraulichen staatlichen Informationen:** Behörden auf Bundes-, Länder- und Gemeindeebene sollten sicherstellen, dass die Daten, die ihnen vorliegen, gegen Bedrohungen aus dem In- und Ausland geschützt sind.

5. **Unterstützung für Innovationen:** Entwickler und Anbieter von innovativen Datensicherheitstools sollten in der Lage sein, technologische Produkte und Tools für die digitale Sicherheit ohne staatliche Vorgaben zu entwerfen.

6. **Verteidigung von kritischen Infrastrukturen:** Anbieter von grundlegenden Versorgungsleistungen wie Banken, Gesundheitsanbieter, Strom- und Wasserversorgungsunternehmen und andere Anbieter von kritischen Infrastrukturen sollten ihren Benutzern die besten Sicherheitstechnologien zur Verfügung stellen können. Zudem sollten flächendeckend Best-Practice-Modelle eingesetzt werden.

7. **Verständnis der weltweiten Auswirkungen:** Kriminelle und terroristische Handlungen machen vor Landesgrenzen nicht Halt. Daher sollten Gesetze und Richtlinien in allen Ländern, in denen Sicherheitstechnologien entwickelt und genutzt werden, eine einheitliche und eindeutige Anwendung finden.

8. **Erhöhte Transparenz:** Vor Einbringung eines Gesetzgebungsvorschlags sollte ein umfassender, transparenter und fundierter Dialog in der Öffentlichkeit über die Zukunft der Technologie und Verschlüsselungstechnologien geführt werden.