Stellungnahme des Cyber Security Cluster Bonn e.V. vom 19.11.2020 zum Entwurf der Resolution des EU-Ministerrats zur Schwächung von Verschlüsselung in Kommunikationsdiensten vom 6.11.2020

Ziel des Cyber Security Cluster Bonn e.V.

Das Ziel des Cyber Security Cluster Bonn e.V. ist es, die Gesellschaft gegen Cyber-Angriffe zu immunisieren und damit die Grundlage für eine sichere Digitalisierung in Deutschland und Europa zu legen. Ein wichtiger Bestandteil dieser Immunisierung ist es, den Einsatz und die breite Anwendung sicherer Kommunikationsdienste zu fördern und dazu beizutragen, dass die von Unternehmen und anderen Institutionen verwendeten Dienste die Schutzziele der Informationssicherheit – Vertraulichkeit, Integrität und Verfügbarkeit – bestmöglich erfüllen.

Aktueller Hintergrund

Als Reaktion auf den Terroranschlag in Wien am 2. November 2020 legte der EU-Ministerrat am 6. November den Entwurf einer Resolution vor, laut der Sicherheitsbehörden und Nachrichtendienste ein einfacherer Zugriff auf verschlüsselte Kommunikation von Messenger-Diensten ermöglicht werden soll. Dazu soll die Verschlüsselung dieser Kommunikationsdienste auf Anordnung umgangen werden können. Die Möglichkeit zu dieser Umgehung soll laut Resolutionsentwurf auf berechtigte staatliche Akteure begrenzt werden, die sich dann im begründeten Notfall über die Betreiber der Dienste Zugriff auf die entschlüsselten Inhalte der Kommunikation verschaffen würden.

Stellungnahme zur Resolution des EU-Ministerrats

Der Cyber Security Cluster Bonn e.V. spricht sich gegen die in dem Resolutionsentwurf geforderten Möglichkeiten zur Schwächung von starker Verschlüsselung in Kommunikationsdiensten aus. Unsere Haltung ergibt sich aus der folgenden Argumentation:

Grundsätzlich ist es sinnvoll, dass befugte staatliche Organisationen in begründeten Fällen und unter Voraussetzungen wie dem Richtervorbehalt das Recht und die Möglichkeit haben, die Privatsphäre zu brechen und Menschen zu überwachen. In der physischen Welt geschieht dies sowohl offen wie auch heimlich. So hat der Staat beispielsweise das Recht und die technischen Mittel, in ein Haus einzubrechen und vor Ort Kameras zu installieren. Die technische Machbarkeit entsteht aus der Tatsache, dass Häuser nicht sicher sind. Ein großflächiger Missbrauch wird durch rechtliche und moralische Aspekte sowie auch durch begrenzte Ressourcen und die Notwendigkeit, für die Installation von Kameras vor Ort zu sein, verhindert.

Eine Übertragung der existierenden Gesetzgebung und Normen in die digitale Welt scheitert allerdings: Nach dem derzeitigen Stand der Technik führt jede Möglichkeit, Verschlüsselung zu umgehen oder zu unterwandern, notwendigerweise zu einer maßgeblichen Schwächung der IT-Sicherheit. Langfristig lässt sich die Nutzung von Hintertüren nicht auf legitimierte Sicherheitsbehörden beschränken. Eine Nutzung durch nicht berechtigte Dritte – bspw. Cyberkriminelle oder fremde Nachrichtendienste – wäre absehbar.

In der digitalen Welt wirken zudem Skaleneffekte, so dass ein großflächiger Missbrauch nicht unterbunden werden könnte. Ebenfalls sind mit dem Internet verbundene Systeme potenziell von jedem Ort der Welt aus angreifbar.

Sofern starke Verschlüsselung im EU-Raum umgangen oder geschwächt würde, könnten Kriminelle ihre Kommunikation anderweitig verschlüsseln und sich somit den Sicherheitsbehörden entziehen. Es ist also höchst zweifelhaft, ob die intendierten Mehrwerte für die berechtigten Stellen überhaupt realisiert werden könnten. Übrig bliebe eine unsichere Kommunikation für die Gesellschaft sowie für private und öffentliche Organisationen.

Ohne starke Verschlüsselung und die Verfügbarkeit zuverlässiger vertraulicher Kommunikationsdienste droht zudem das Vertrauen der Gesellschaft sowie auch der Privatwirtschaft in die Sicherheit digitaler Dienste zu erodieren. Dieses Vertrauen ist jedoch Voraussetzung für eine erfolgreiche Digitalisierung, insbesondere auch in hochsensiblen Bereichen wie der medizinischen Versorgung, in behördlichen Bürgerdiensten oder auch in der Kommunikation zwischen Anwälten und ihren Mandanten.

Die Schaffung von Möglichkeiten, Verschlüsselung zu unterwandern, steht dem von der Bundesregierung in der Digitalen Agenda erklärten Ziel entgegen, Deutschland bei der privaten Kommunikation in der Breite zum „Verschlüsselungsstandort Nr. 1“ auf der Welt zu machen.

Empfehlungen

Zum effektiven Schutz der Gesellschaft vor Terrorismus und Kriminalität bei gleichzeitiger Ermöglichung sicherer Kommunikation sprechen wir folgende Empfehlungen aus.

Bevor Pläne zur Integration von Hintertüren oder Schwächung von kryptographischen Systemen konzipiert werden, sollten transparente Untersuchungen der erhofften Vorteile und befürchteten Nachteile durchgeführt werden. Es sollten insbesondere folgende Fragen beantwortet werden können:

- Wie viele Straftaten oder Terroranschläge hätten in der Vergangenheit durch Hintertüren bzw. eine Schwächung starker Verschlüsselung verhindert werden können?
- Wie viele und welche Art von Straftaten würden durch die Schwächung starker Verschlüsselung und den potenziellen Zugriff unberechtigter Dritter auf unverschlüsselte Kommunikationsdaten ermöglicht?
- Wie viele und welche Art von Kriminellen würden nach Schwächung starker Verschlüsselung auf andere, stark verschlüsselte Kommunikationslösungen ausweichen?
- Welche technischen Möglichkeiten können entwickelt werden, die eine Absicherung und Überwachung von in Kommunikationsdiensten eingebauter Hintertüren erlauben würden?
- Welche anderen Möglichkeiten bestehen, die Effektivität von Ermittlungen und Kriminalitäts-Prävention im Cyber-Raum zu steigern? Lassen sich beispielsweise Ausstattung und Ausbildung der Ermittler verbessern?

Fazit

Es sollte ein produktiverer Dialog bzgl. verschiedener Konzepte zu Möglichkeiten der Strafverfolgung und Prävention im digitalen Raum stattfinden. Dogmatische Forderungen oder Ablehnungen einzelner Konzepte sollte es nicht geben. Nach dem heutigen Stand der Technik sind die Nachteile der Schwächung starker Verschlüsselung vielfältig belegt. Der Einbau von Hintertüren und Schwachstellen in verschlüsselte Kommunikation ist daher abzulehnen.