totemo Statement

Hintertüren für Ende-zu-Ende-Verschlüsselung: Ein enormer Vertrauensverlust wäre die Folge

Von: Marcel Mock, CTO, totemo AG

Zürich-Flughafen, 17. November 2020 – Die Regierungschefs der Europäischen Union führen aktuell Gespräche darüber, ob und wie ihre Behörden in Zukunft verschlüsselte Kommunikation abhören und in die Strafverfolgung einbeziehen können. Verschiedene Medien berichteten in den vergangenen Tagen, dass die Hersteller von Apps wie WhatsApp oder Signal dazu bewogen werden sollen, die Ende-zu-Ende-Verschlüsselung in ihren Produkten aufzuweichen. Polizei und Nachrichtendiensten soll ein sogenannter „Generalschlüssel" zur Verfügung gestellt werden, mit dem sie unter bestimmten Bedingungen und ausnahmsweise Zugriff auf den Inhalt der Nachrichten erlangen könnten. Bis jetzt existiere keine rechtliche Grundlage dafür, dass Behörden Einblicke in verschlüsselte Online-Chats erzwingen können, schreibt die „Neue Zürcher Zeitung".

Die Rufe von staatlicher Seite nach einer Aushebelung oder einem Verbot von Verschlüsselungs-Techniken sind nicht neu. In den USA läuft seit den neunziger Jahren ein Streit, die „Crypto Wars", um Bestrebungen der Bundesregierung, die private Verschlüsselung von Daten zu unterbinden. In diesem Zusammenhang kam beispielsweise Apple 2016 ins Visier des FBI. Die Behörde forderte vom IT-Unternehmen Zugang zu einem gesperrten iPhone, Apple weigerte sich, diesen zu gewährleisten. 2019 wurden Forderungen nach dem Zugang zu Chat-Nachrichten auch im deutschen Innenministerium laut. Datenschützer, Politiker und Cybersecurity-Experten kritisieren die Pläne zum Einbau von Hintertüren in Kryptographie scharf.

Die Idee ist nobel, doch der Weg ist der falsche

Das Bestreben der Strafverfolgungsbehörden, Straftaten aufzuklären und möglicherweise sogar verhindern zu können, ist verständlich; ebenso wie die Notwendigkeit, dazu auch Nachrichten von Instant Messengern auszuwerten. Auch wäre es grundsätzlich möglich, die Ende-zu-Ende-Verschlüsselung mit einem Generalschlüssel für die Behörden zu versehen. Dennoch ist von solchen Plänen entschieden abzuraten. Ein staatlicher Ausnahme-Zugang würde die Verschlüsselung und den Schutz der Privatsphäre grundsätzlich schwächen, da Angreifer – etwa Hacker, Geheimdienste, oder autoritäre Staaten – jetzt nur noch an einer zentralen Stelle ansetzen müssten, um an die Schlüssel zu gelangen.

Das Konzept der Verschlüsselung würde damit unterwandert: Wenn beispielsweise zwei Kommunikationspartner (von insgesamt vielen Millionen möglichen Kommunikationspartnern) miteinander verschlüsselt kommunizieren, und einer der beiden Schlüssel kompromittiert wird, dann wäre der Schaden vergleichsweise gering. Wenn der Generalschlüssel kompromittiert würde, wäre das ein kryptografischer Super-GAU, denn die Angreifer erhielten auf einen Schlag Zugang zu allen Inhalten. Staatliche und Geschäftsgeheimnisse wären nicht mehr sicher.

Dass der staatliche Zugang wahrscheinlich nicht exklusiv wäre, sieht man etwa daran, dass staatliche Organe selbst immer wieder Hackerangriffen zum Opfer fallen. Staaten haben sich in der Vergangenheit nicht gerade durch besonders sichere Infrastrukturen ausgezeichnet. Daher ist die Gefahr gross, dass sie nicht in der Lage wären, den Generalschlüssel zu schützen. Ausserdem: Was grundsätzlich möglich ist, weckt Begehrlichkeiten. Auch wenn die Geheimdienste verschiedener Länder beispielsweise bei der Terrorismusbekämpfung miteinander kooperieren, heisst das noch lange nicht, dass sie bei wirtschaftlichen Interessen im Gleichklang agieren.

Ein Generalschlüssel würde grundsätzlich Zugang zu allen Informationen bieten und Wirtschaftsspionage vereinfachen. Die Folge wäre ein enormer Vertrauensverlust, der die Digitalisierung gefährden und hemmen könnte. Viele Bürger wären vermutlich zögerlicher in Bezug auf Digitalisierungsvorhaben, wenn den Behörden ein Generalschlüssel für verschlüsselte Inhalte und Systeme zu Verfügung stünde, gerade bei Projekten der öffentlichen Hand.

Wie die Europäische Union beim Thema Verschlüsselung weiter verfahren wird, ist noch offen. Der Vorschlag der EU-Regierungschefs ist laut NZZ so weit vorberaten, dass schon Anfang Dezember ein Beschluss der Innen- und der Justizminister verabschiedet werden könnte. Die Politiker sind gut beraten, im Sinne von Datenschutz, Cybersicherheit und einer zukunftssicheren Digitalisierung zu entscheiden.

Über totemo

Der Schweizer Softwarehersteller totemo ag bietet Lösungen für den sicheren Austausch geschäftlicher Informationen. totemo schützt E-Mail-Kommunikation und Datentransfer durch Verschlüsselung und legt dabei besonderen Wert auf optimale Nutzerfreundlichkeit – natürlich auch auf mobilen Geräten. Die patentierte und FIPS-140-2-validierte totemo-Sicherheitsplattform ermöglicht eine schnelle und einfache Integration in jede bestehende IT-Infrastruktur.

Weltweit vertrauen mehr als 3.5 Millionen Nutzer in 1‘500 Unternehmen und Organisationen über alle Branchen hinweg auf die Sicherheitslösungen von totemo, darunter namhafte Grosskonzerne.

Weitere Informationen unter: www.totemo.com oder folgen Sie uns auf Twitter: @totemoag.

Kontakt zum Unternehmen:
totemo ag
Diana Eisenberg
The Circle 9
8058 Zürich-Flughafen
Tel: +41 44 914 99 00
diana.eisenberg@totemo.com

Kontakt für die Presse:
Jenni Kommunikation
Oliver Schneider
Südstrasse 85
8008 Zürich
Tel.: +41 44 388 60 80
oliver.schneider@jeko.com