Secomba GmbH

Werner-von-Siemens-Str. 6
86159 Augsburg
Deutschland

T 0049 (0) 821 90786150
www.boxcryptor.com
info@boxcryptor.com

Sitz der Gesellschaft
Augsburg, HRB 26138
Amtsgericht Augsburg

Geschäftsführung
Andrea Pfundmeier
Robert Freudenreich

Positionspapier

Ende-zu-Ende-Verschlüsselung schützen

10. November 2020

Zusammenfassung

Vertrauliche Kommunikation ist eine Grundstütze unserer freiheitlich - demokratischen Gesellschaft und muss deshalb unbedingt erhalten bleiben

Ende-zu-Ende-Verschlüsselung gerät immer dann unter Beschuss, wenn komplexe Probleme mit einfachen Mitteln bekämpft werden sollen. Terror und Kindesmissbrauch sind schreckliche Verbrechen, müssen jedoch an ihren Wurzeln bekämpft werden. Die IT-Sicherheit aller Bürger und Bürgerinnen dafür aufzugeben, ist unverhältnismäßig.

Forderungen

Freie Meinungsäußerung und das Recht auf Privatsphäre der gesamten Bevölkerung dürfen nicht angetastet werden, um einzelne Straftäter und Straftäterinnen zu belangen.

Bitte beachten Sie dazu unsere drei Forderungen:

- Forderung 1: Straftaten an der Ursache bekämpfen und vorbeugende Maßnahmen ergreifen statt auf Vorratsdatenspeicher und Algorithmen als Allheilmittel zu setzen.

- Forderung 2: Verwischung zwischen Strafverfolgung und Zivilgesellschaft verhindern.

- Forderung 3: Strafverfolgungsbehörden finanziell und personell besser ausstatten, Behörden besser vernetzen.

Was ist Ende-zu-Ende-Verschlüsselung?

Viele Anbieter von Internetdiensten verschlüsseln die hochgeladenen Inhalte ihrer Nutzer und Nutzerinnen. Das ist Bestandteil des Service – seien das nun Cloud-Speicher, Chat-Dienste oder Banking-Apps. Solange jedoch die Instanz, welche die Verschlüsselung durchführt, auch in Besitz des Schlüssels ist, können die Anbieter jederzeit auf die Inhalte zugreifen. In den USA können sie sogar durch Behörden dazu gezwungen werden, Inhalte unverschlüsselt herauszugeben. Das wird im sogenannten CLOUD Act geregelt.

Bei Ende-zu-Ende-Verschlüsselung verschlüsselt jeder Nutzer oder jede Nutzerin ihre Inhalte selbst und teilt den Schlüssel nur mit anderen, berechtigten Personen. So kann man sichergehen, dass ausschließlich diese berechtigten Personen Zugriff auf die Klartext-Dateien erhalten.

Ende-zu-Ende-Verschlüsselung ist zum Beispiel notwendig, um sicher zu kommunizieren, Geschäftsgeheimnisse zu schützen oder um die Anforderungen der DS-GVO an den Schutz personenbezogener Daten zu erfüllen.

Wodurch wird Ende-zu-Ende-Verschlüsselung bedroht? Aktuelle Diskussionspunkte

In den USA wurden mit dem EARN IT Act und dem LAED Act zwei Gesetze auf den Weg gebracht, die Ende-zu-Ende-Verschlüsselung de facto verbieten wollen. Anbetracht der Tatsache, dass die meisten großen Anbieter von Internetdiensten in den USA sitzen, betrifft dieses Verbot dann auch eine große Anzahl von EU-Bürgern und -Bürgerinnen.

Mittlerweile gibt es aber auch innerhalb der Europäischen Union Stimmen, die ein ähnliches Gesetz wie den EARN IT Act fordern. Zu nennen sind da der Anti-Terror-Koordinator der EU Gilles de Kerchove und die EU-Innenkommissarin Ylva Johansson.

Gibt es technische Lösungen?

Indem Anbieter direkt beim Datei-Upload nach behördlich bekannten Hashes (mathematischen Abdrücken) von illegalem Bild- und Video-Material suchen, können solche Dateien vor der Veröffentlichung erkannt und gemeldet werden.

Dieses Verfahren funktioniert allerdings nur, wenn die Hashes der Dateien nicht verändert werden. Ende-zu-Ende-Verschlüsselung nimmt jedoch eine Änderung vor, wodurch eine automatische Überprüfung nutzlos wird. Dieses Problem kann nur gelöst werden, indem man die starke Verschlüsselung „aufweicht".

Allerdings gibt es kein Verfahren, welches eine „abgeschwächte" Variante von Ende-zu-Ende-Verschlüsselung erlaubt – eine Abschwächung ist gleichbedeutend mit einer Abschaffung. Dies geht auch deutlich aus dem Papier hervor, mit dem die EU-Kommission die Diskussion um die Ende-zu-Ende-Verschlüsselung eröffnet hat: Man kann Ende-zu-Ende-Verschlüsselung nur beibehalten oder abschaffen.

Forderungen

Freie Meinungsäußerung und das Recht auf Privatsphäre der gesamten Bevölkerung dürfen nicht angetastet werden, um einzelne Straftäter und -täterinnen zu belangen. Unsere drei Forderungen:

Forderung 1: Straftaten an der Ursache bekämpfen und vorbeugende Maßnahmen ergreifen statt auf Vorratsdatenspeicher und Algorithmen als Allheilmittel zu setzen.

Als Grund für die Abschaffung von Ende-zu-Ende-Verschlüsselung werden immer wieder zwei Motive genannt: der Schutz vor Terror und die Strafverfolgung von Personen, die Missbrauchsdarstellungen von Kindern im Internet teilen und sammeln. Für beide Probleme gibt es wirksame vorbeugende Maßnahmen aus verschiedenen Fachbereichen. Wir plädieren dafür, die Ursachen zu bekämpfen und Fachorganisationen besser auszustatten, anstatt auf Überwachung und Vorratsdatenspeicherung zu setzen.

Forderung 2: Verwischung zwischen Strafverfolgung und Zivilgesellschaft verhindern.

Derzeit werden in Deutschland Unternehmen im Rahmen des NetzDG dazu gezwungen, vermeintlich gesetzeswidrige Kommentare zu löschen. Die Entscheidung, ob ein Kommentar gesetzeswidrig ist, wird deshalb von Algorithmen und

Angestellten der jeweiligen Unternehmen getroffen statt von Strafverfolgungsbehörden. Bei Straftaten wie Volksverhetzung mag das möglich sein. Doch bei komplizierten Sachverhalten wie Beleidigung entscheiden selbst Gerichte oft unterschiedlich. Das führt dazu, dass Plattformen eher zu viel löschen als zu wenig, denn Strafen für versehentlich gelöschte Inhalte gibt es nicht.

Bereits nach kurzer Zeit haben die Regierungen von Weißrussland, Indien, Malaysia und Russland das NetzDG kopiert. Ein negativer Exportschlager, wie Prof. Dr. Wolfgang Schulz das Gesetz nennt.

Für verschlüsselte Inhalte ein ebensolches Verfahren zu installieren muss unbedingt verhindert werden. Unternehmen mit privatwirtschaftlichen Interessen dürfen nicht zum Arm von Regierungen und Strafverfolgungsbehörden gemacht werden.

Forderung 3: Strafverfolgungsbehörden finanziell und personell besser ausstatten, Behörden besser vernetzen.

Verstärkt durch die Vorratsdatenspeicherung, aber auch schon davor, hören wir immer wieder Klagen von der Polizei, dass die schiere Flut an Arbeit nicht zu bewältigen ist. Unattraktive Arbeitsplätze sorgen zudem für einen Fachkräftemangel in den IT-Abteilungen der Polizeibehörden. Mit zunehmender Digitalisierung werden auch die „Internet-Verbrechen“ eher mehr als weniger. Wir fordern Nachrüstung und Personalaufstockung.

Mangelnde Vernetzung der Strafverfolgungsbehörden in unterschiedlichen Ländern und Bundesländern hat in der Vergangenheit mehrfach zu Ermittlungspannen geführt. Hier sind Verbesserungen notwendig und eine Anpassung des Föderalismus an das digitale Zeitalter dringend angeraten.

Fazit

Die Ermittlungen bei Terror und Kindesmissbrauch werden stets als Grund genannt, um Ende-zu-Ende-Verschlüsselung abzuschaffen. Unserer Ansicht nach müssen die Verbrechen Einzelner bekämpft werden, nicht die Privatsphäre aller.