Bundeskriminalamt

Zusammenfassung

Bund-/Ländererhebung der RETASAST zum polizeifachlichen Bedarf an der Überwachung und Auswertung verschlüsselter Telekommunikationsinhalte

Erhebungszeitraum:
01. Januar 2012 – 31. Dezember 2013

BKA

KI 15 RETASAST

1. Anonymisierung und Kryptierung von Telekommunikation

Telekommunikation ist der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen (§ 3 Nr. 22 TKG). Durch die Entwicklungen im Bereich der Informations- und Kommunikationstechnologien, insbesondere in den Bereichen Anonymisierung und Kryptierung, läuft die „klassische" Telekommunikationsüberwachung („TKÜ", Überwachung der Telekommunikation durch Ermittlungsbehörden im Rahmen ihrer gesetzlichen Befugnisse mittels Ausleitung der Daten durch den Telekommunikationsanbieter) zunehmend ins Leere. Das liegt daran, dass der Ursprung der Telekommunikation in Form des genutzten physikalischen Anschlusses bzw. des Urhebers häufig nicht mehr ermittelt werden kann (Folge der Anonymisierung) und ein zunehmend hoher Anteil der Telekommunikation nicht mehr überwach- bzw. auswertbar ist (Folge der Verschlüsselung).

Dabei ist darauf hinzuweisen, dass verschlüsselte Kommunikation mittlerweile in vielen Fällen keine willentliche Nutzung einer Kryptierungssoftware voraussetzt, sondern zunehmend von den gängigen elektronischen Kommunikationsanbietern als technischer Standard verwendet wird. Darüber hinaus integrieren die Anbieter der gängigsten (mobilen) IuK-Plattformen (z.B. Apple, Google) inzwischen Ende-zu-Ende-Verschlüsselungsverfahren in ihre Systeme, die die Kommunikation automatisch verschlüsseln. Insofern muss inzwischen ein signifikanter Teil dieser Kommunikation über die allgemein gebräuchlichen Anbieter aufgrund ihrer Verschlüsselung als nicht mehr auswertbar durch die Ermittlungsbehörden angesehen werden.

2. Quellen-TKÜ

Damit durch die Nutzung von Kommunikationsverschlüsselung kein strafverfolgungsfreier Raum entsteht, benötigen die Ermittlungsbehörden Ausgleichsmaßnahmen, um die wachsenden Lücken bei der klassischen Telekommunikationsüberwachung zu schließen.

Ein möglicher Lösungsansatz ist, die Kommunikationsdaten vor der Verschlüsselung (bzw. nach Entschlüsselung) aufzuzeichnen und an die Ermittlungsbehörden zu übertragen (sog. Quellen-Telekommunikationsüberwachung; Quellen-TKÜ). Die Verschlüsselung kann so umgangen werden. Hierzu ist erforderlich, eine spezielle Software auf das zur Kommunikation genutzte Endgerät aufzubringen.

Die verdeckte bzw. heimliche Aufbringung der Software auf das Endgerät stellt für die Sicherheitsbehörden eine besondere technische Herausforderung dar und ist regelmäßig mit hohem Aufwand verbunden.

Ob die Durchführung von Quellen-TKÜ im Ermittlungsverfahren auf der Grundlage des § 100a, b StPO in der aktuellen Fassung zulässig ist, wird in Rechtsprechung, Literatur und Praxis nicht einheitlich beurteilt. BMI und BKA vertreten die Auffassung, dass die Befugnisnormen §§ 100a, b StPO bereits nach derzeitiger Rechtslage die Anordnung und Durchführung einer Quellen-TKÜ zulassen. Auch die Innen- und Justizressorts der Länder erachten h.W. §§ 100a, b StPO als taugliche Rechtsgrundlage für Quellen-TKÜ und erwirkten in der Vergangenheit entsprechende Anordnungen.
Der Generalbundesanwalt hingegen ist der Auffassung, §§ 100a, b StPO genügten den vom Bundesverfassungsgericht in seinem Urteil zur Online-Durchsuchung vom 27.02.2008 aufgestellten Vorgaben nicht und beantragt daher keine entsprechenden Maßnahmen beim Ermittlungsrichter des Bundesgerichtshof. Folglich ist die Durchführung von Quellen-TKÜ in Ermittlungsverfahren des BKA (ST), die unter der Sachleitung des Generalbundesanwaltes laufen, nicht möglich.

Im Rahmen der präventivpolizeilichen Aufgaben des BKA zur Abwehr von Gefahren des internationalen Terrorismus ist die Quellen-TKÜ, neben der TKÜ, für das BKA bereits explizit in § 20l Abs. 2 BKAG als zulässige Eingriffsmaßnahme vorgesehen. Die dafür notwendige und den Datenschutzanforderungen genügende Überwachungssoftware wird voraussichtlich im Laufe des Jahres 2015 (wieder) zur Verfügung stehen.

Dabei ist es aus Sicht des BKA nicht ausreichend, diese Software ausschließlich im Bereich der Gefahrenabwehr zum Einsatz zu bringen. Vielmehr soll die mit hohem personellem und finanziellem Aufwand entwickelte Software auch bei der Strafverfolgung als Einsatzmittel zur Verfügung stehen. Um auch in diesen Fällen entsprechende Handlungs- und Rechtssicherheit bei der Beantragung, Anordnung und Durchführung der Quellen-TKÜ in Bund und Ländern zu schaffen, sieht BKA es als geboten an, die StPO um eine klarstellende, explizite Befugnis für Quellen-TKÜ zu ergänzen. Diese Forderung hat auch Eingang in den Koalitionsvertrag für die 18. Wahlperiode gefunden. Zudem wurde mit Beschluss des 69. Deutschen Juristentages vom 20.09.2012 der fachliche Bedarf bestätigt und der Gesetzgeber aufgefordert, eine (klarstellende) Regelung zum Einsatz von Quellen-TKÜ im Rahmen der Strafverfolgung zu schaffen.

3. Kernaussagen der Bund-/Ländererhebung der RETASAST zum polizeifachlichen Bedarf an der Überwachung und Auswertung verschlüsselter Telekommunikationsinhalte

3.1. Hintergrund

Konsens in der 237. Sitzung des AK II am 10./11.04.2013 war, dass der polizeifachliche Bedarf an der Quellen-TKÜ sowie mögliche Ausgleichsmaßnahmen weiterhin belegt werden müssen. Daher wurde das BKA gebeten, geeignetes rechtstatsächliches Fallmaterial, das Ermittlungsdefizite in Folge der rechtlich/technisch nicht möglichen Überwachung oder Auswertung verschlüsselter Telekommunikationsinhalte belegt, in Bund und Ländern regelmäßig zu erheben.

Hieraus sollen Empfehlungen und Argumente für die politischen Entscheidungsträger im Hinblick auf eine rechtspolitische Diskussion zur Erforderlichkeit von Rechtsänderungen (Ausgleichsmaßnahmen) abgeleitet werden. Es handelt sich insofern um eine Zusammenstellung und qualitative Auswertung von tatsächlichen Einzelsachverhalten (Rechtstatsachen) und nicht um eine quantitative Vollerhebung.

3.2. Datenbasis

Die Bund-/Ländererhebung wurde beim Bundeskriminalamt (KI15-RETASAST) nach Zustimmung des BMI vom 20.06.2013 bis zum 15.01.2014 durchgeführt und bezog sich auf Verfahren aus dem Erhebungszeitraum: 01.01.2012 bis 31.12.2013. Aktiv beteiligten sich 17 der 19 gewonnenen Erhebungsteilnehmer (16 Bundesländer, BPol, ZKA und BKA).

Gemeldet wurden 292 Verfahren im Bereich der Schwerkriminalität (siehe hierzu § 100a-StPO-Katalogtaten), in denen das BKA, das ZKA, die BPol oder die Länder Ermittlungsdefizite hinnehmen mussten, weil die Überwachung oder Auswertung verschlüsselter Telekommunikationsinhalte rechtlich/technisch nicht möglich war.

Zu den vorliegenden Erhebungsergebnissen können nach Abschluss der Erhebung kurz gefasst folgende inhaltliche Aussagen getroffen werden:

- Schwerpunktmäßig betroffene Deliktsfelder

  Bei der Auswertung werden die Verfahren den jeweils betroffenen Deliktsbereichen in Anlehnung an den Straftatenkatalog des § 100a StPO zugeordnet. 53 % der gemeldeten Fälle lassen sich dem Deliktsbereich „Rauschgiftkriminalität“ zuordnen. Einen weiteren Schwerpunkt stellt der Bereich Eigentums- und Vermögensdelikte/ Betrugsdelikte/Raub/Erpressung (einschließlich Computerbetrug) mit rund 23 %

gemeldeten Fälle dar. Insgesamt sind in den Verfahren oftmals mehrere Deliktsbereiche betroffen (Mehrfachzählung eines Verfahrens daher möglich).

- Art schwerpunktmäßig genutzter Kryptierungsdienste

  Bei der Auswertung der Verfahren nach Art der genutzten Kryptierungsdienste wurde in den meisten Fällen die Verwendung sog. Instant-Messenger (rund 72 %) sowie kombinierter VoIP-/Instant-Messenging-Programme (rund 59 %) beim überwachten Anschluss festgestellt. Mindestens eine dieser beiden relativ ähnlichen Kategorien im Hinblick auf die Kommunikationsformen „Telefonie und (Kurz-) Nachrichten" wurde in rund 97 % der Fälle festgestellt. Dies zeigt die signifikant häufige Verwendung derartiger Kryptierungsdienste in den hier ausgewerteten Fällen. Zudem wurde auch häufig (in rund 40 %) die Nutzung mehrerer bzw. weiterer Dienste, wie Anonymisierungsdienste, VPN oder Browserverschlüsselungen, erkannt (auch hier Mehrfachzählung möglich).

- Nutzungs- und Verbreitungsgrad der Kryptierungsmöglichkeiten

  Die Erfahrungen aus den in Bund und Ländern geführten Ermittlungsverfahren zeigen, dass die Täter immer häufiger miteinander über Internetdienste kommunizieren und dabei verschiedene Anonymisierungs- und Verschlüsselungsmethoden (Instant-Messaging-Dienste, VoIP, VPN, Proxy-Server, u. a.) zum Teil ganz bewusst einsetzen: In rund 72 % der Fälle kann die Nutzung von Kryptierungsdiensten technisch belegt werden. Ferner führen in rund 67 % der Fälle belegbare Absprachen der Tatverdächtigen zu der Vermutung, dass im konkreten Fall kryptiert kommuniziert wurde. Ein konspiratives Täterverhalten findet sich besonders stark ausgeprägt in Phänomenbereichen, die von einem arbeitsteiligen, organisierten und vernetzten Zusammenwirken von Mittätern gekennzeichnet sind, mithin bei jeglichen Formen der Organisierten Kriminalität und in vielen Bereichen des Terrorismus. Hier sind oft detaillierte Kenntnisse über die Grenzen polizeilicher Ermittlungsmaßnahmen vorhanden – kryptierte Kommunikationsmittel werden gezielt und absprachegemäß genutzt, um einer (möglichen) staatlichen Überwachungsmaßnahme zu entgehen und die eigene Identität zu verschleiern.

  Auf Seiten der Täter ist ein hohes Innovationspotential sowie im zunehmenden Maße eine Nutzung der sich ständig verbessernden technischen Möglichkeiten (verschlüsselte, zumeist kostengünstige, praktikable, nutzerfreundliche und innovative Telekommunikationsdienste) festzustellen. Kommunikations- und Kryptierungsmöglichkeiten variieren stetig und können von den Ermittlungsdienststellen

zunehmend mit den bislang zur Verfügung stehenden Mitteln nur schwer bzw. überhaupt nicht mehr erkannt oder überwacht werden.

- Erkennbare erhebliche Ermittlungsdefizite

  Die nicht auswertbaren Telekommunikationsinhalte führten - unabhängig davon, ob sie unbewusst oder gezielt von den Kommunikationsteilnehmern verursacht worden sind - zu teils erheblichen Überwachungslücken und damit zu unvollständiger Ermittlungsergebnissen, einer mangelhaften Beweislage oder gar zum Scheitern der Ermittlungen. Insbesondere die Aufklärung der Kommunikations- und Organisationsstrukturen der Tatverdächtigen sowie die Planung und Durchführung von (Begleit-)Ermittlungsmaßnahmen werden in erheblichem Maße erschwert. Gleichzeitig gehen Versuche, die Ermittlungsdefizite auch nur im Ansatz auszugleichen, in der Regel mit deutlich intensiveren Grundrechtseingriffen bei den Betroffenen einher.