Generalstaatsanwaltschaft Frankfurt am Main
- Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) -
Außenstelle Gießen

HESSEN

Deutscher Bundestag
18. Wahlperiode
Ausschuss für Wirtschaft und Energie

Ausschussdrucksache 18(9)1282
26. Juni 2017

Generalstaatsanwaltschaft -ZIT- • Ostanlage 7 • 35390 Gießen

Aktenzeichen **420 E 65/17**

Ausschuss für Wirtschaft und Energie

Deutscher Bundestag
Platz der Republik 1
10117 Berlin

Bearbeiter: OStA May
Durchwahl: (0641) 934 - 3653
Fax: (0641) 934 - 3659

Datum: 25.06.2017

Gesetzentwurf der Bundesregierung
Entwurf eines Dritten Gesetzes zur Änderung des Telemediengesetzes - Drucksache 18/12202 -

Stellungnahme der Zentralstelle zur Bekämpfung der Internetkriminalität

I. Ausgangslage:

Der Entwurf eines Dritten Gesetzes zur Änderung des Telemediengesetzes (3. TMGÄndG) stellt u.a. klar, dass WLAN-Betreiber nicht verpflichtet werden dürfen, Nutzer vorab zu registrieren, die Eingabe eines Passwortes zu verlangen oder das Anbieten des Dienstes gänzlich einzustellen (§ 8 Abs. 4).
Grund für den Verzicht auf jedwede Sicherungs- und Registrierungspflichten beim Betrieb von öffentlichen und privaten WLAN-Hotspots ist nach Auffassung der Bundesregierung einerseits, dass eine Verpflichtung zur Erhebung von Bestandsdaten erhebliche gesetzliche Pflichten im Hinblick auf Umgang und Schutz dieser personenbezogenen Daten und damit einen Aufwand mit sich bringen würde, der viele potentielle Anbieter von einer WLAN-Bereitstellung abschrecken würde. Andererseits soll verhindert werden, dass nach der EuGH-Entscheidung in der Rechtssache McFadden WLAN- Betreiber ihr Netz der Öffentlichkeit aus Angst vor Abmahnungen oder hoheitlichen Anordnungen nicht zur Verfügung stellen wollen.
Welche Auswirkungen dieses Bestreben der Bundesregierung, durch eine flächendeckende Bereitstellung von WLAN-Hotspots ohne Pflicht zur Registrierung und Erhebung von Nutzungsdaten auf Belange der Strafverfolgungsbehörden haben kann, soll nachfolgend skizziert werden.

II. Telekommunikationsüberwachung als wesentlicher Eckpfeiler effektiver Strafverfolgung

Die Telekommunikationsüberwachung (TKÜ) stellt im Bereich der Strafverfolgung ein wichtiges, wenn auch besonders eingriffsintensives Ermittlungsinstrument dar. Während bislang TKÜ- Maßnahmen insbesondere durch die stark zunehmende Verschlüsselung des Datenverkehrs erschwert wurden, zieht die flächendeckende Zur-Verfügung-Stellung von registrierungsfreien und ungesicherten WLAN-Hotspots eine der TKÜ vorgelagerte, gravierendere Problematik nach sich.

Die Überwachung eines Internetzugangs erfolgt anschlussbezogen auf dem physikalischen Übertragungsweg. Die Inanspruchnahme von WLAN-Hotspots ermöglicht einem Nutzer nicht nur einen Internetzugang an beliebigen Orten, sondern auch die Möglichkeit, über diese zu telefonieren (Wifi-Calling). Wenn für die Nutzung keine oder keine im Vorfeld ermittelbaren Zugangsdaten verwendet werden, führt dies zu einer vollständigen Anonymisierung des Nutzers. Dessen zur Einwahl genutztes, mobiles Endgerät ist nicht identifizierbar. Damit steht für die Ausfertigung einer Anordnung zur Umsetzung einer regulären anschlussbezogenen TKÜ kein technisches Merkmal (Kennung) zur Verfügung.

Auch eine Überwachung des (gesamten) Hotspots zur Ermittlung einer Kennung ist nicht erfolgversprechend. Neben der Tatsache, dass es höchst unwahrscheinlich ist, dass Täter zur Begehung von Straftaten immer denselben Hotspot nutzen, ist zu beachten, dass Betreiber von Telekommunikationsanlagen, an die weniger als 10.000 Teilnehmer angeschlossen sind, keine technischen und organisatorischen Vorkehrungen zur Umsetzung von TKÜ-Maßnahmen treffen müssen und das Einbringen polizeieigener Technik (auch mit Einverständnis des Hotspot-Betreibers) sowohl aus zeitlichen als auch ermittlungstaktischen Erwägungen (Aufdeckungsgefahr) ausscheiden dürfte.

Während bei Überwachung und Aufzeichnung der Telekommunikation bereits heute (insbesondere durch Verschlüsselung) Überwachungslücken bestehen und daraus Erkenntnisdefizite für die Strafverfolgung bis hin zur Wirkungslosigkeit der TKÜ resultieren, könnte die zu erwartende, stark zunehmende Verfügbarkeit offener WLANs dazu führen, dass eine Wirkungslosigkeit der TKÜ generell eintritt, denn die zur Einwahl genutzten mobilen Endgeräte sind mehr identifizier- und damit auch nicht mehr überwachbar.

Eine Verschärfung der derzeitigen Situation liegt darüber hinaus auch darin begründet, dass durch das vermehrte Angebot offener WLANs die Gelegenheit zur täterseitigen anonymen Nutzung zukünftig vervielfältigt wird. Zudem dürfte die derzeit ggf. noch ansatzweise gegebene Hemmschwelle, die bei einer Nutzung eines öffentlich zugänglichen WLANs zur Abwicklung beweiserheblicher Telekommunikation besteht, weiter gesenkt oder sogar gänzlich beseitigt werden.

III. Widerspruch zu den gesetzgeberischen Maßnahmen zur Verbesserung der Aufklärung von Straftaten unter Nutzung von Telekommunikationsmitteln

Der Verzicht auf jedwede Sicherungs- und Registrierungspflichten steht zudem in klarem Widerspruch zu den in jüngerer Zeit vorgenommenen, vielfältigen gesetzgeberischen Maßnahmen, Straftaten unter Nutzung von Telekommunikationsmitteln besser aufklären zu können. Es steht darüber sogar zu befürchten, dass diese Maßnahmen durch die Einführung registrierungsfreier WLAN-Hotspots wirkungslos bleiben könnten.

1. Registrierungspflicht bei Prepaid-Produkten (Kundendaten)

Die Erfolgschancen von Cyberermittlungen steigen mit zunehmender Qualität der durch die Diensteanbieter zur Verfügung gestellten Daten.
Während den von den geschäftsmäßigen Erbringern von Telekommunikationsdiensten gem. § 111 TKG zu erhebenden Kundendaten bei Festverträgen durchaus eine hohe Validität zu bescheinigen ist, ergaben Stichprobenuntersuchungen der Bundesnetzagentur im Segment der im Voraus bezahlten Mobilfunkdienste eine enorme Anzahl offensichtlich fehlerhafter Datensätze in Kundendatenbanken von Anbietern von Telekommunikationsdiensten. Es lagen zahlreiche Hinweise auf automatische und händisch eingetragene systematische Generierungen von fiktiven Angaben vor, sodass die die Auskunftsverfahren der Behörden nach den §§ 112, 113 TKG in vielen Verfahren zu keinen brauchbaren Informationen führen bzw. keinen Anknüpfungspunkt für weitere Ermittlungen liefern.
Da diese verschleiernde Nutzung von PrePaid-Karten bei der Kommunikation in kriminellen und terroristischen Strukturen nach Einschätzung des Gesetzgebers ein erhebliches Sicherheitsrisiko darstellt, das die Aufklärung von Netzwerkstrukturen erheblich erschwert, hat er mit der ab dem 01.07.2017 geltenden Verpflichtung zur Datenverifizierung („Ausweispflicht") bei Mobilfunkverträgen durch das Gesetz zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus reagiert und damit die Qualität dieser „Vertragsdaten" deutlich erhöht.

Wenn aber die Falschregistrierung bei Providern, die eine Identifizierung des Nutzers zwar erschwert, aber (durch dessen providerseitige Anbindung) nicht unmöglich macht, bereits als erhebliches Sicherheitsrisiko bewertet wird, so muss die Frage erlaubt sein, ob das Risiko nicht um ein Vielfaches höher einzuschätzen ist, wenn Straftäter künftig ohne jegliche Registrierung und damit ohne jede Möglichkeit der Identifizierung über wechselnde, offene WLANs kommunizieren oder Straftaten begehen können.

2. Vorratsdatenspeicherung gem. § 100g Abs. 2 StPO (Verkehrsdaten)

Im Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (BTDrs 18/5088) hat der Gesetzgeber festgestellt, dass bei der Aufklärung schwerer Straftaten Verkehrsdaten ein wichtiges Hilfsmittel für die staatlichen Behörden sind. Denn die (unveränderte) IP-Adresse weist jedenfalls auf den Anschluss hin, der für eine Straftat in Anspruch genommen wurde.
Die völlig uneinheitliche Speicherpraxis der Diensteanbieter machte es jedoch nahezu vom Zufall abhängig, ob Verkehrsdaten zum Zeitpunkt der Anfrage noch vorhanden waren oder nicht. Dies führte häufig dazu, dass Ermittlungsverfahren erfolglos verliefen, da retrograde, täterseitig genutzte IP-Adressen nicht mehr erhoben werden konnten und der einzig erfolgversprechende Ermittlungsansatz waren.
Da dieser Zustand mit dem Gebot einer effektiven Strafverfolgung nur schwer zu vereinbaren war, hat der Gesetzgeber mit dem ab 01.07.2017 umzusetzenden § 100g Abs. 2 StPO eine Verpflichtung der Telekommunikationsanbieter geschaffen, Verkehrsdaten für eine beschränkte Zeit zu speichern und die Erhebung der Daten durch staatliche Stellen unter sehr strengen Voraussetzungen ermöglicht.
Da jedoch Anbieter, die ihren Kunden nur eine kurzzeitige Nutzung des Telekommunikationsanschlusses ermöglichen, nicht unter die gem. § 113a TKG zur Speicherung von Vorratsdaten Verpflichteten fallen (BTDrS 18/5088, S. 37), wird das durch die Einführung der Vorratsdatenspeicherung beabsichtigte Ziel, durch eine (nahezu) lückenlose Speicherung von Verkehrsdaten schwere Straftaten aufklären zu können, nicht erreicht werden können, wenn potentielle Täter massenhaft und flächendeckend auf Hotspots zurückgreifen können, deren Betreiber keinerlei Speicherverpflichtung unterliegen.

Überdies könnte die verdachtsbegründende Eigenschaft von Verkehrsdaten völlig entfallen. Wird durch den Zugriff auf Verkehrsdaten bspw. festgestellt, dass über einen Hotspot Kinderpornographie verbreitet wurde, so wäre zunächst völlig unklar, ob die Verbreitung durch eine (unbekannten) Hotspot-Nutzer oder mglw. durch dessen Betreiber selbst erfolgt ist.

3. Funkzellenabfrage gem. § 100g Abs. 3 StPO (Verkehrsdaten)

Bei der Funkzellenabfrage werden alle Verkehrsdaten erhoben, die in einer bestimmten Funkzelle angefallen sind, um festzustellen, welche Mobilgeräte zu einer bestimmten Zeit der betreffenden Funkzelle zuzuordnen waren. Die Maßnahme eignet sich insbesondere zur Aufklärung von Serientaten (z.B. Sexualdelikte, Wohnungseinbrüche). Dabei steigt die Erfolgswahrscheinlichkeit bei der Aufklärung von mit ähnlichem Modus Operandi ablaufenden Taten an unterschiedlichen Orten mit zunehmender Anzahl signifikant an. Denn hierbei werden die Datenbestände, die aus den jeweiligen Funkzellenabfragen stammen, in einem „cross-over-Verfahren" miteinander abgeglichen. Tauchen Kennungen wiederholt auf, so deutet das darauf hin, dass die dahinter stehenden Personen als Tatverdächtige in Betracht kommen können.
Der Gesetzgeber hat für dieses wichtige Ermittlungsinstrumentarium – unter strengen Voraussetzungen – auch den Zugriff auf Vorratsdaten ermöglicht.
Der Erfolg der Maßnahme setzt allerdings voraus, dass alle in einer Funkzelle befindlichen mobilen Endgeräte auch providerseitig erfasst sind.
Nutzt der Täter einen privaten WLAN-Hotspot zur Kommunikationsaufnahme, loggt er sich gerade nicht in einem Mobilfunkmast eines (geschäftsmäßigen) Providers ein, sodass eine Funkzellenabfrage erfolglos bleiben wird.

4. Quellen-TKÜ und Onlinedurchsuchung (Inhaltsdaten)

Laut Medienberichten hat der Bundestag am 22.06.2017 die gesetzlichen Grundlagen für die Anwendung einer Quellen-TKÜ sowie der Online-Durchsuchung geschaffen. Eine gesetzliche Regelung zur Quellen-TKÜ musste geschaffen werden, da der Datenverkehr –insbesondere über Messenger-Dienste – heute nahezu flächendeckend providerseitig verschlüsselt wird. Überwachungsmaßnahmen gem. § 100a StPO waren daher in zunehmendem Maß nicht mehr möglich; die Inhalte der Kommunikation konnten nicht mehr erfasst werden.

Hintergrund der Schaffung einer gesetzlichen Grundlage zur Online-Durchsuchung ist, dass die von den Tätern genutzten Endgeräte immer häufiger vollverschlüsselt sind und daher nicht ausgewertet werden können.

Beide wichtigen Ermittlungsinstrumentarien setzen jedoch voraus, dass das Endgerät identifiziert ist. Eine solche Identifizierung ist aber – wie oben ausgeführt – bei der registrierungsfreien Nutzung eines WLAN-Hotspots nicht möglich, sodass zu befürchten steht, dass beide Maßnahmen ins Leere laufen könnten.

5. Fazit

Bereits heute entstehen im Rahmen der Durchführung von Maßnahmen der TKÜ erhebliche Überwachungslücken und damit Erkenntnisdefizite für die Strafverfolgung, wenn sich Täter zur Abwicklung beweiserheblicher Telekommunikation oder zur Begehung von Straftaten wechselnder öffentlicher WLANs bedienen. Eine erhöhte Verfügbarkeit öffentlicher WLANs und deren zu erwartende Nutzung wird zwangsläufig dazu führen, dass sich diese Überwachungslücken vergrößern werden und damit die TKÜ als wesentliches Ermittlungsinstrument zunehmend wirkungslos wird. Die vom Gesetzgeber geschaffenen Rechtsgrundlagen zur Verbesserung der Aufklärung von Straftaten unter Nutzung von Telekommunikationsmitteln könnten bei flächendeckender Verfügbarkeit öffentlicher Hotspots nahezu vollständig ins Leere laufen.

III. Gefährdung der Netzsicherheit und des WLAN-Betreibers

Die anonyme Nutzung offener WLAN-Hotspots erleichtert zudem Angriffe auf die Sicherheit des Netzes (bspw. durch massenhafte Verbreitung von Schadsoftware). War diese Verbreitung bislang überwiegend nur durch den Einsatz von Botnetzen möglich, so ermöglichen in großer Anzahl verfügbare offene Hotspots die Verbreitung von Malware, ohne dass es eines Botnetz-Einsatzes bedarf. Es steht daher zu befürchten, dass es zukünftig zu zunehmenden Angriffen auf die Netzsicherheit kommen wird.
Nicht unterschlagen werden darf auch, dass das Zur-Verfügung-Stellen eines Hotspots auch für dessen Betreiber nicht unerhebliche Risiken mit sich bringt. So erhöht sich das Risiko, dass sein System kompromittiert wird, ganz erheblich. Hat er keine Registrierung des Schädigers vorgenommen und dessen Zugangsdaten nicht gespeichert, wird dieser nicht ermittelbar sein.

IV. Lösungsansatz

Um die Begehung von Straftaten unter Nutzung von freien, anonymen WLAN-Zugängen, aber auch mögliche Gefahren für den Betreiber und den Nutzer wirkungsvoll eindämmen zu können, wären eine verifizierbare Registrierung im WLAN und eine für einen definierten Zeitraum festgelegte Speicherung von WLAN-Nutzungsdaten durch den WLAN-Betreiber mit der anschließenden Möglichkeit der Nutzung dieser Daten zur Identifizierung der Täter die einzig erfolgversprechenden Maßnahmen, das Problem des Missbrauchs einzudämmen.

Die Arbeitsgruppe 2 „Neue Erfassungsansätze und TKÜ-Regulierung“ des Runden Tisches des BMI zur „Sicherstellung der Telekommunikationsüberwachung in der Zukunft“ hat in ihrem Abschlussbericht vom 04.03.2014 eine umfassende Beschreibung der „Problemfelder Nomadisierung und Anonymisierung“ vorgenommen und konkreten Handlungsbedarf aufgezeigt.

Sie hat im Wesentlichen festgestellt, dass eine handhabbare, lückenlose Überwachungsfähigkeit der Individualkommunikation nur umgesetzt werden könne, wenn gleichzeitig eine personenbezogene Kennung für alle Nutzer vorgeschrieben würde und die Betreiber aller WLAN-Hotspots sowie sämtlicher Internetcafès zur Nutzung dieser Kennungen und zur Vorhaltung von TKÜ-Technik verpflichtet würden.

Allerdings erscheint der Arbeitsgruppe die Einführung einer personalisierten Kennung („Internetausweis“), die eine anonyme Nutzung des Internets nicht mehr ermöglichen und das Recht auf informationelle Selbstbestimmung massiv einschränken würde, ebenso wenig realistisch wie eine Verpflichtung von Betreibern, an deren Anlagen nur wenige Teilnehmer angeschaltet sind, Überwachungstechnik vorzuhalten.

Alternativ wurde daher die Verpflichtung zur Implementierung einer technisch einfach zu realisierenden Schnittstelle (mirror port) in der Anlage des Betreibers diskutiert, mit der sichergestellt werden könnte, dass zumindest nach notwendigen Vorermittlungen und vor Ort eine Überwachungsmöglichkeit besteht. Auch wurde angedacht, ob die Anlage sowie die Signalisierung zum dahinter liegenden Internetzugangsanbieter so verändert werden kann, dass vergebene Nutzerkennungen an den dahinter liegenden Internetzugangsanbieter weitergereicht werden können.

Aus hiesiger Sicht erscheint auch die Durchsetzbarkeit dieser alternativen Handlungsempfehlungen wenig realistisch. Diese machen jedoch deutlich, wie schwierig es erscheint, Strafverfolgungsinteressen einerseits und eine vertretbare Belastung des Betreibers öffentlicher Hotspots in Einklang zu bringen.

Gleichwohl darf diese Problematik aus hiesiger Sicht nicht dazu führen, auf Sicherungs- und Registrierungspflichten, die mit einfacher, auf dem Markt bereits verfügbarer, kostengünstiger Technik umgesetzt werden könnte, gänzlich zu verzichten.

May
Oberstaatsanwalt