OESTERREICHISCHE COMPUTER GESELLSCHAFT®
AUSTRIAN COMPUTER SOCIETY

An das
Bundesministerium für Justiz
Museumstraße 7
1070 Wien

per E-Mail:
team.s@bmj.gv.at
begutachtungsverfahren@parlament.gv.at

Wien, am 21. August 2017

Stellungnahme der OCG zum Ministerialentwurf eines Bundesgesetzes, mit dem die Strafprozessordnung 1975 geändert wird (Strafprozessrechtsänderungsgesetz 2017) – 325/ME

Die OCG erlaubt sich zunächst, sich selbst vorzustellen:

Die **Österreichische Computer Gesellschaft (OCG)** ist ein gemeinnütziger Verein, der 1975 zur Förderung der Informatik und der Kommunikationstechnologie unter Berücksichtigung ihrer Wechselwirkungen mit Mensch und Gesellschaft gegründet wurde. Die OCG hat rund 1.400 Mitglieder und versteht sich als Plattform, um Gesellschaft, Wissenschaft und Wirtschaft im Sinne der Förderung der Informatik zu vernetzen. Um IT-Kompetenz zu fördern und zu zertifizieren, bietet die OCG verschiedene Produkte und Leistungen an, u.a. seit 1997 als nationale Zertifizierungsstelle den ECDL (den Europäischen Computerführerschein).

Neben dem IT-Ausbildungsschwerpunkt liegt ein großer Fokus im IT-Security- und im Datenschutz-Bereich: Die OCG betreibt eine akkreditierte Zertifizierungsstelle für die ISO/IEC 27001-Norm, dem Standard für die Zertifizierung von Informationssicherheits-Managementsystemen (ISMS). Der Verein bietet darüber hinaus in rund 25 Arbeitskreisen (wie dem Forum Privacy, dem Forum e|Government und den Arbeitskreisen IT-Security sowie Rechtsinformatik) **ExpertInnen aus Wissenschaft, Wirtschaft, Verwaltung und Zivilgesellschaft** die Möglichkeit zum Austausch von Forschungsergebnissen, Best Practices sowie zum kritischen Diskurs.

Die OCG nimmt zum vorliegenden Entwurf wie folgt Stellung:

Zunächst ist anzumerken, dass bereits der **Zeitpunkt der Begutachtung** eines derart sensiblen Entwurfs im Hochsommer höchst bedenklich ist, da dadurch ein kollaboratives Verfassen und Abstimmen einer Stellungnahme erheblich erschwert wird, insbesondere innerhalb einer verhältnismäßig großen und gegliederten Organisation, deren Fachexpertinnen und Fachexperten sich ehrenamtlich beteiligen. Die OCG hat sich daher entschieden, eine verhältnismäßig kurze Stellungnahme abzugeben, die vor allem an technischen Aspekten anknüpft und leider nicht alle kritikwürdigen Punkte abdecken kann. **Aus dem Umstand, dass die OCG nicht zu allen vorgeschlagenen Maßnahmen Stellung nimmt, ist daher nicht zu schließen, dass sie die übrigen Maßnahmen befürwortet.**

OESTERREICHISCHE COMPUTER GESELLSCHAFT
AUSTRIAN COMPUTER SOCIETY

Grundsätzlich ist zu den vorliegenden Plänen der Bundesministerien für Justiz und für Inneres Folgendes zu sagen: Die OCG beobachtet mit Sorge eine **fortlaufende Ausweitung staatlicher Überwachungsbefugnisse**, deren Nutzen für die Kriminalitätsbekämpfung und Aufrechterhaltung der öffentlichen Sicherheit viel zu häufig fragwürdig bleibt. Eine Begründung der Erforderlichkeit und Eignung der Maßnahmen auf Basis einer **wissenschaftlichen Auseinandersetzung** mit der Sicherheitslage in Österreich und den zu erwartenden Auswirkungen der vorgeschlagenen Maßnahmen liegt nicht vor. Es bedarf daher dringend einer evidenzbasierten Sicherheitspolitik auf Basis einer **Überwachungsgesamtrechnung**[1] zur Evaluierung der Wirksamkeit und der Folgen bestehender und geplanter Überwachungsgesetze. Die OCG ist gerne bereit, sich insbesondere mit technischer Expertise an einem solchen Prozess zu beteiligen.

Zur Auskunft über den PUK-Code (§ 76a Abs. 1 StPO-E):

Die Erläuterungen **begründen sachlich nicht, zu welchem Zweck** von der Auskunft über Stammdaten nach § 76a Abs. 1 StPO künftig auch die vom Anbieter vergebene Nummer, die dem Teilnehmer die Überwindung der Sperre der persönlichen Identifikationsnummer des Benutzers ermöglicht (PUK-Code), umfasst sein soll.

Anders als bei Stammdaten handelt es sich dabei nicht um eine identifizierende Information bzw. um eine Information, die Aufschluss über den Teilnehmer gibt, sondern der PUK dient dem Zugriff auf Informationen, die auf der SIM-Karte gespeichert sind. Warum man die Herausgabe dieser Information an keine weitere Bedingung knüpft als an ein **bloßes Ersuchen der kriminalpolizeilichen Behörden**, ist daher ebenso wenig nachvollziehbar wie die diesbezüglichen Ausführungen in den Erläuterungen.

Die OCG lehnt daher diesen Vorschlag ab, zumindest solange eine einleuchtende sachliche Begründung fehlt.

Zur Beschlagnahme von Briefen (§ 135 Abs. 1 StPO-E):

Das Abfangen von Briefen, Paketen und anderen Postsendungen war bisher sehr eng beschränkt auf Fälle, in denen sich der Beschuldigte wegen einer Straftat in Haft befindet oder seine Vorführung oder Festnahme deswegen angeordnet wurde. **Ohne eine triftige Begründung** oder eine vorherige Ankündigung durch die Bundesregierung, die eine öffentliche Diskussion ermöglicht hätte, soll diese Einschränkung nun ersatzlos entfallen. **Eingriffe in das Briefgeheimnis würden damit massiv ausgeweitet**. Ebenso soll § 137 Abs. 2 StPO gestrichen werden, sodass die sinngemäße Anwendung der §§ 111 Abs. 4 und 112 entfallen würde und damit die Pflicht, die Betroffenen innerhalb von 24 Stunden über die Durchführung der Maßnahme zu informieren. Dadurch würde der **Rechtsschutz massiv eingeschränkt und das Vertrauen in die Postzustellung erschüttert** werden. Wenn eine Sendung nicht ankommt, würde künftig stets Unsicherheit darüber herrschen, ob die Post dafür verantwortlich ist oder die Sendung beschlagnahmt wurde.

Aus den genannten Gründen ist der Vorschlag in der vorliegenden Form abzulehnen.

[1] Wie das deutsche Bundesverfassungsgericht (BVerfG) ausgesprochen hat (BvR 256/08 u.a. vom 2.3.2010, Rz. 218), kann eine staatliche Überwachungsmaßnahme bzw. deren Verhältnismäßigkeit nur in Zusammenschau mit anderen, bereits bestehenden Befugnissen beurteilt werden. Für eine solche Zusammenschau und Gesamtevaluierung hat sich der Begriff Überwachungsgesamtrechnung etabliert.

Zum Einsatz von IMSI-Catchern (§ 135 Abs. 2a StPO-E):

Mit § 135 Abs. 2a StPO-E soll eine eigenständige und ausdrückliche Grundlage für den Einsatz von IMSI-Catchern für den Bereich der Strafverfolgung geschaffen werden. Die OCG weist darauf hin, dass der **Funktionsumfang eines IMSI-Catchers i.d.R. über die Möglichkeit der Lokalisierung eines Mobilfunkgeräts hinausgeht**. Ist der IMSI-Catcher einmal im Einsatz, ist die Versuchung für Ermittler – aus Gründen, die aus deren Sicht verständlich sind – groß, auch andere Funktionen zu nutzen, wie insbesondere das Mithören von Gesprächen (Inhaltsüberwachung). Die Regelung müsste daher Sicherheitsmaßnahmen enthalten, die geeignet sind, dies wirksam zu verhindern und den **Einsatz von IMSI-Catchern faktisch auf das gesetzlich Zulässige zu beschränken**.

Hinsichtlich der Notwendigkeit einer richterlichen Bewilligung der staatsanwaltschaftlichen Anordnung besteht eine **Diskrepanz zwischen dem Entwurf und der Textgegenüberstellung**: Im Entwurf (Punkt 18) ist eine gerichtliche Bewilligung vorgesehen, während in der Textgegenüberstellung in § 137 Abs. 1 und § 138 Abs. 5 der Einsatz des IMSI-Catchers ausdrücklich vom Erfordernis einer richterlichen Bewilligung ausgenommen ist. Die OCG spricht sich angesichts der Eingriffsintensität des IMSI-Catchers dringend für das **Erfordernis einer richterlichen Bewilligung** aus. Die Eingriffsintensität entspricht mindestens jener einer Standortbestimmung i.S.v. § 134 Z 2 StPO (§ 92 Abs. 3 Z 6 TKG) und der in den Erläuterungen offenbar vorgenommene Vergleich mit § 53 Abs. 3b SPG hinkt, da dieser ausschließlich auf Akutsituationen beschränkt ist, in der eine gegenwärtige Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen besteht.

Darüber hinaus ist auf die Problematik im Zusammenhang mit der Verständigungspflicht der Betroffenen nach Beendigung der Maßnahme gemäß § 138 Abs. 5 StPO-E hinzuweisen. Der Kreis der Betroffenen kann technisch nicht auf die „Zielperson(en)“ reduziert werden. Der **Einsatz eines IMSI-Catchers betrifft potenziell eine große Zahl von Personen** in seinem Umkreis. Deren **Verständigung erfordert jedoch einen weiteren Eingriff in ihre Grundrechte**, nämlich die Ermittlung ihrer Identität, d.h. ihrer Stammdaten. Dies wäre so umzusetzen, dass den Behörden die Identität dieser „zufällig“ Betroffenen nicht bekannt wird, beispielsweise indem die Verständigung über die Durchlaufstelle abgewickelt wird. Im Entwurf ist dies jedoch nicht vorgesehen und möglicherweise gar nicht bedacht worden.

Schließlich ist allgemein anzumerken, dass IMSI-Catcher aufgrund ihres Funktionsprinzips die Möglichkeit aller Mobilfunkteilnehmer in ihrer Umgebung beeinflussen können, Anrufe zu tätigen und zu empfangen. Es kann daher die Situation eintreten, dass Menschen aufgrund des behördlichen Einsatzes eines IMSI-Catchers nicht oder nur verzögert in der Lage sind, einen Notruf abzusetzen.

Aus den genannten Gründen lehnt die OCG die angeführten Bestimmungen in der vorliegenden Fassung ab.

Zum staatlichen Einsatz von Schadsoftware – „Bundestrojaner“ (§ 135a StPO-E):

Die OCG hält es für ein legitimes Anliegen, verschlüsselte Chats Verdächtiger unter denselben Voraussetzungen wie SMS und Telefonate zu überwachen, wenn dies der Prävention und Aufklärung schwerer Straftaten dient, mit vertretbaren Mitteln möglich ist und die Verhältnismäßigkeit gewahrt bleibt. Die OCG hält es jedoch nicht für legitim, dass auch die **Überwachung von Geräten beliebiger Dritter** erlaubt werden soll, mit denen ein Verdächtiger kommunizieren könnte, wie das aktuell in § 135a Abs. 1 Z 3 lit. b a.E. StPO-E geplant ist. Das beträfe nämlich jede beliebige Person, mit der ein Verdächtiger Kontakt aufnehmen könnte.

Österreichische Computer Gesellschaft | Wollzeile 1 | 1010 Wien | Tel: +43 (0)1 512 02 35-0 I Fax: DW 9 I info@ocg.at I www.ocg.at
UID-Nr.: ATU 36822300 DVR-Nr.: 0406856 ZVR-Nr.: 125 777 049 I Zertifiziert nach Qualitätsnorm ISO 9001:2008

Ausdrücklich ist dabei an Personen zu denken, die an den kriminellen Aktivitäten des Verdächtigen völlig unbeteiligt sind, denn ansonsten könnten sie ohnedies selbst als Verdächtige überwacht werden. Eine wahrscheinliche Zielgruppe für den Einsatz dieser Bestimmung zur Überwachung von Geräten Dritter sind wohl Verwandte und Freunde des Verdächtigen. Die Kommunikation des Verdächtigen mit diesen Personen könnte z.B. Aufschluss über seinen Aufenthaltsort geben und somit für Ermittler von Interesse sein. Bedenkt man nun folgende technische Gesichtspunkte, gelangt man zu der Vermutung, dass **Ermittler sogar viel häufiger solche unbeteiligte Dritte überwachen könnten als die Verdächtigen selbst**. Die Installation einer Schadsoftware ist nämlich umso einfacher, je älter das Gerät, genauer gesagt die installierte Betriebssystemversion ist, denn ältere Betriebssystemversionen enthalten mehr bekannte Sicherheitslücken als neuere. Auf solchen Geräten kann Schadsoftware auf Basis allgemein bekannter Sicherheitslücken installiert werden, die vom Hersteller in späteren Betriebssystemversionen bereits geschlossen wurden. Insbesondere bei Smartphones mit dem am weitesten verbreiteten Betriebssystem Android ist die Verbreitung älterer und teilweise völlig veralteter Betriebssystemversionen sehr hoch.[2] Somit kann prognostiziert werden, dass Ermittler auf Basis der geplanten Bestimmung des § 135a Abs. 1 Z 3 lit. b a.E. StPO-E **im Umfeld eines Verdächtigen gezielt nach Personen mit älteren Geräten suchen könnten**, um auf diesen die Schadsoftware zu installieren. Dies ist verhältnismäßig einfach und unterliegt nicht den technischen und finanziellen Einschränkungen wie die Installation auf der modernsten Gerätegeneration. Wie diese Überlegungen zeigen, **könnte der Einsatz von Schadsoftware durch Ermittlungsbehörden künftig deutlich mehr Menschen treffen**, als man zunächst annimmt, und zwar vor allem unbeteiligte Dritte, deren Geräte technisch nicht auf dem aktuellsten Stand sind, wobei so gut wie jeder solche Menschen in seinem Umfeld hat.

Die **Folgen** des geplanten § 135a StPO-E gehen aber über die eben beschriebene Betroffenheit beliebiger einzelner Dritter noch deutlich hinaus und **treffen tatsächlich die Gesamtbevölkerung**. Anstatt für mehr Sicherheit zu sorgen, gefährden die Pläne zum staatlichen Einsatz von Schadsoftware unsere Sicherheit, nämlich die **Sicherheit von Computersystemen**, die weltweit millionenfach genutzt werden – auch in Krankenhäusern, (selbstfahrenden) Fahrzeugen, in der Justiz und von der Polizei. Erst kürzlich wurde gemeldet, dass für die österreichische Polizei tausende iPhones und iPads beschafft werden.[3]

Die einzig denkbare Variante zur Überwachung von WhatsApp und ähnlichen Chatprogrammen wäre es, die **Kommunikation vor der Verschlüsselung oder nach der Entschlüsselung abzufangen**. Die **Verschlüsselung selbst ist bei vertrauenswürdigen Produkten nicht zu knacken**. Das ist wünschenswert, denn sonst wäre dies auch Kriminellen und Diktaturen möglich.

Es muss daher eine spezielle Software am Gerät installiert werden, die man aus technischer Sicht völlig zu Recht als Schadsoftware oder „Bundestrojaner“ bezeichnen kann. Unwahrscheinlich ist, dass die Polizei für die Installation vorübergehend das Smartphone des Verdächtigen in die Hände bekommt. Daher bleibt nur die Ferninstallation. Die Polizei könnte versuchen, Verdächtige mit gefälschten E-Mails dazu zu bringen, sich durch Klick auf einen interessant klingenden Link die Software unabsichtlich selbst zu installieren. Auch diese Variante ist in einem Rechtsstaat strikt abzulehnen. Wenn in jeder behördlichen Nachricht ein Bundestrojaner versteckt sein könnte, schadet das dem Vertrauen in die

[2] Siehe z.B. https://www.golem.de/news/android-verbreitung-nougat-knackt-die-10-prozent-marke-1707-128790.html.
[3] Siehe http://derstandard.at/2000061808554/Polizisten-erhalten-tausende-iPhones-und-eigenen-Messenger.

staatlichen Institutionen und konterkariert Österreichs jahrzehntelange Bemühungen, Vorreiter im E-Government zu sein.

Wenn die zu überwachende Person nichts von der Ferninstallation der Überwachungssoftware merken soll, kann diese nur **über eine Sicherheitslücke per Fernzugriff eingeschleust** werden. Damit beschreitet der Staat denselben Weg wie Kriminelle, die Systeme über ebensolche Lücken mit Schadsoftware infizieren. Laut Studien werden allein die durch Erpressungssoftware weltweit verursachten Schäden im Jahr 2017 etwa fünf Milliarden US-Dollar ausmachen. Der Erpressungstrojaner „WannaCry", der im Mai 2017 enorme Schäden anrichtete (u.a. auch in Krankenhäusern), nützte nachweislich eine Sicherheitslücke, die der US-Geheimdienst NSA mehr als fünf Jahre lang selbst ausnutzte, anstatt sie an Microsoft zu melden, damit diese in allen Windows-Systemen behoben werden kann. Wenn Staaten und deren Softwarezulieferer Wissen über Sicherheitslücken erwerben, horten und ausnutzen, anstatt sie an die Hersteller der betroffenen Systeme zu melden, werden sich die Berichte über durch Trojaner verursachte Schäden häufen. **Die vorgeschlagene Maßnahme ist somit eine Maßnahme zur Förderung der Internetkriminalität.**

Auch der laut den Erläuterungen geplante **Audit zur Sicherstellung der Beschränkung des Programms auf die gesetzlich vorgesehenen Funktionen ist zu hinterfragen**. Vorauszuschicken ist, es ist nicht anzunehmen, dass Österreich diese Software selbst entwickelt, denn ohne Kooperation mit Herstellern von Schad- und Spionagesoftware (oder alternativ mit anderen Staaten) ist Österreich wohl nicht in der Lage, ausreichend Informationen über Sicherheitslücken zu erlangen, wie sie für die unbemerkte Installation der Software erforderlich sind. Hersteller von Schad- und Spionagesoftware für den staatlichen Einsatz werden nicht dazu bereit sein, den Quellcode ihrer Software für einen Audit offenlegen. In den Erläuterungen ist daher auch nur ein Audit der Architektur der Software, nicht jedoch des Programmcodes erwähnt. Ein Audit des Programmcodes wäre allerdings unabdingbar, um tatsächlich feststellen zu können, welche Funktionalität die Software vorsieht und welche nicht. Die gewissermaßen zweitbeste Lösung wäre ein Audit der fertigen Software selbst, also ein umfassender Benutzungstest, doch auch ein solcher ist in den Erläuterungen nicht erwähnt, geschweige denn im vorgeschlagenen Gesetzestext.

Doch zu bezweifeln ist nicht nur, dass die Beschränkung des Programms auf die gesetzlich vorgesehenen Funktionen festgestellt werden kann, sondern auch, dass eine solche Beschränkung überhaupt möglich ist. **Es ist technisch äußerst schwierig bis unmöglich, die intendierte Funktionalität des Programms von einer Online-Durchsuchung abzugrenzen**, welche ausdrücklich nicht zulässig sein soll, was von der OCG begrüßt wird. Zu bedenken ist auch, durch Aufbringen einer Schadsoftware an sich wird in der Regel bereits derart intensiv in ein System eingegriffen, dass auch andere Komponenten des Systems unweigerlich davon betroffen sind. Aus dem Wort „oder" in § 135a Abs. 2 Z 1 ergibt sich, dass das Programm auch eine **dauerhafte Schädigung oder Beeinträchtigung des Computersystems herbeiführen darf**, solange das Programm nach Beendigung der Ermittlungsmaßnahme funktionsunfähig ist.

Hinzu kommt, bei der Installation der Schadsoftware aus der Ferne ist es nur eingeschränkt möglich, sicherzustellen**, dass das angegriffene Gerät tatsächlich jenes ist, das von der Maßnahme getroffen werden soll**. Erschwerend wirkt sich hierbei aus, dass die Online-Durchsuchung, die Aufschluss darüber

OESTERREICHISCHE COMPUTER GESELLSCHAFT®
AUSTRIAN COMPUTER SOCIETY

geben könnte, nicht erlaubt sein soll.[4] Kriminelle können Mittel ergreifen, um diese Unsicherheit auszunützen und die Behörden hinsichtlich der Zielgeräte bewusst in die Irre zu führen. Auch unter diesem Gesichtspunkt ist daher zu bezweifeln, dass diese Maßnahme in der Praxis so zielgerichtet ist, wie es dargestellt wird.

Zusammenfassend ist zu sagen, der Einsatz einer Schadsoftware zum Abgreifen vor der Verschlüsselung oder nach der Entschlüsselung ist das einzige derzeit bekannte Mittel zum „Abhören" wirksam Ende-zu-Ende-verschlüsselter Kommunikation. Wenngleich die OCG das zugrundeliegende Anliegen teilt, Kommunikation von Personen, die schwerer Straftaten verdächtig sind, abhören zu können, wäre es nach Auffassung der OCG **aufgrund der dargelegten Probleme und Kollateralschäden für die Allgemeinheit äußerst unverhältnismäßig**, dieses Mittel einzusetzen. In einem Rechtsstaat ist es geradezu eine Selbstverständlichkeit, dass **Ermittler zur Erreichung grundsätzlich legitimer Ziele nicht jedes Mittel einsetzen dürfen**. Mit dem Einsatz staatlicher Spionagesoftware wäre diese rote Linie, insbesondere wegen der dargelegten unumgänglichen und nicht eingrenzbaren Gefährdung Dritter, klar überschritten.

Für die Österreichische Computer Gesellschaft

Dipl.-Ing. Wilfried Seyruck
Präsident

Dr. Ronald Bieber
Generalsekretär

Dipl.-Ing. Dr. Walter Hötzendorfer
Co-Leiter OCG Forum Privacy

[4] Umgekehrt betrachtet ist dies ein weiterer Aspekt, warum Quellen-Telekommunikationsüberwachung, wie sie hier intendiert ist, und Online-Durchsuchung, die hier nicht intendiert ist, nicht zu trennen sind.