Stellungnahme zu dem Ministerialentwurf 325/ME betreffend Bundesgesetz, mit dem die Strafprozessordnung 1975 geändert wird

der Fachschaft Informatik der TU Wien im Sinne des HSG § 20 Abs. 4

21. August 2017

Obwohl sich Europa in der nachweislich längsten friedlichen bzw. kriegsfreien Ära seiner Geschichte befindet [1], versuchen politische Gruppierungen und Strömungen seit Jahren, die Bevölkerung immer stärker zu überwachen. Anstatt Ursachen für (kriminelles) Verhalten zu beseitigen - etwa Armut als Ursache für Beschaffungskriminalität, Gesetzeslücken als Ursachen für Steuerhinterziehung, soziale und ökonomische Unsicherheit als Ursache für Radikalisierung - werden überzogene Sicherheits- und Überwachungsinstrumente implementiert.

Resultat sind Gewöhnungseffekte, Selbstzensur, und Umgehungsverhalten. Der französische Philosoph Michel Foucault hat dafür den Begriff "Panoptismus" geprägt: Unabhängig davon, ob eine Überwachung tatsächlich stattfindet, diszipliniert sich das womöglich unter Beobachtung stehende Individuum selbst. Es passt sein Verhalten an die gestellten normativen Erwartungen an. Hält der Zustand über einen längeren Zeitraum an, führt dieser Mechanismus zu einer Verinnerlichung der Normen. Aus einem (für den_die Normaufsteller_in) kostenintensiven Fremdzwang wird ein kostengünstiger Selbstzwang (Selbstdisziplinierung) [2].

Insgesamt sind uns bei der Durchsicht der Unterlagen - Gesetzesentwurf, Textgegenüberstellung, Vorblatt & Folgenabschätzung sowie Erläuterungen - einige Probleme aufgefallen. Entsprechend der Informationen aus der Problemanalyse (Folgeabschätzung) erscheint uns, abgesehen von ihrer kompletten Überzogenheit, auch die Platzierung einiger Maßnahmen in der StPO als komplett falsch. Wer unbedingt die gesamte Bevölkerung unter den Generalverdacht des Erwerbs illegaler Waren im Darknet stellen möchte, sollte dies eher im SPG machen. Einige vorgeschlagene Maßnahmen befinden sich in einer rechtlichen bzw. ethischen Grauzone, etwa die Zusammenarbeit mit Sicherheitsfirmen, die Sicherheitslücken finden und verkaufen, anstatt sie den Software-Hersteller_innen bekannt zu machen - diese Vorgehensweise bedeutet eine Gefährdung aller Benutzer_innen der betroffenen Software auf Staatskosten.

Die Behauptung, "ohne die vorgeschlagenen Änderungen würde die Effektivität der Strafverfolgung abnehmen", ist für uns nicht nachvollziehbar. Laut Daten des BMI hat sich die Aufklärungsquote in den vergangenen Jahren stetig verbessert (43,2 % im 1.

Halbjahr 2011, 44 % im Jahr 2015, 45,9 % im Jahr 2016)[3, 4, 5]. Hier redet das Innenministerium seine eigene Arbeit schlecht, um unnötige, überzogene Maßnahmen zu argumentieren.

Die Einschätzung, dass das BMI in der Lage wäre, die "Entwicklung […] der Überwachungssoftware iZm verschlüsselten Nachrichten" selbst zu übernehmen, zweifeln wir stark an. Die Kostenaufstellung in der Folgenabschätzung lässt dann auch eher den Schluss zu, dass das BMI die Software zur Gänze von externen Dienstleister_innen zu erwerben plant (Lizenzgebühren, aber keine Personalressourcen in der Kostenaufstellung).

Empfehlung: Aufgrund **massiver Bedenken** datenschutzrechtlicher, gesellschaftlicher, menschenrechtlicher, ethischer sowie technischer Natur empfehlen wir das **komplette Verwerfen** des vorliegenden Entwurfs.

Außerdem empfehlen wir den für den Entwurf verantwortlichen Personen die Lektüre von Cory Doctorow's "Little Brother" im Speziellen sowie seine Arbeit im Allgemeinen. Der Autor macht seine Werke selbst auf seiner Website [3] (kostenlos bzw. gegen Spende) zugänglich. Wir regen an, das Buch eingehend zu lesen und nicht nur kurz zu überfliegen, um die Kernaussagen zu begreifen. Unserer Erfahrung nach hilft gemeinsames Lesen und Diskutieren von neuen Inhalten, etwa gemeinsam mit den Kolleg_innen vom Ministerium für Inneres, beim tiefergehenden Verständnis und nachhaltigen Erfassen.

[1] https://ec.europa.eu/germany/eu60/frieden_de
[2] Michel Foucault: *Überwachen und Strafen – Die Geburt des Gefängnisses.* Frankfurt/M. 1992
[3] http://www.bmi.gv.at/cms/bk/publikationen/krim_statistik/files/2011/krim_stat_juli_2011.pdf
[4] http://www.bmi.gv.at/cms/BK/publikationen/krim_statistik/2015/1342016_Web_Sicherheit__2015.pdf
[5] http://www.bmi.gv.at/cms/BK/publikationen/krim_statistik/2016/Web_Sicherheit_2016.pdf
[6] http://craphound.com/littlebrother/download/

Herausgabepflicht für PUK, § 76a (1)

Kaum jemand braucht einen PUK jemals. Dieser Code wird benutzt, um die SIM-Karte zu entsperren, nachdem der PIN-Code zu oft falsch eingegeben wurde [1]. Das ist nur möglich, wenn das Gerät zur Hand ist. Wofür genau Polizei, Gericht oder Staatsanwaltschaft einen PUK-Code brauchen, ist unklar. Zum Entsperren eines Displays wird jedenfalls kaum ein PIN-Code, der dem der SIM-Karte entspricht, benutzt (SIM-PINs sind üblicherweise vierstellig; zum Sperren eines Handy-Displays

werden kaum weniger als 6 Stellen erlaubt). Um das Display zu entsperren, gibt es ein gelinderes Mittel - welches, wann immer möglich, anzuwenden ist: die Entfernung der SIM-Karte aus dem Gerät.

Empfehlung: Der Grund sowie die Sinnhaftigkeit dieser Maßnahme sind unbekannt. Entsprechend empfehlen wir, die Maßnahme ersatzlos zu streichen.

[1] https://de.wikipedia.org/wiki/Personal_Unblocking_Key

IMSI-Catcher - Lokalisierung einer technischen Einrichtung, § 135 (2a)

Der Einsatz eines IMSI-Catchers geht aufgrund der technischen Voraussetzungen weit über die bloße Lokalisierung des anvisierten Gerätes hinaus. Einerseits ermöglicht er tatsächlich das Abhören von Gesprächen - in diesem Fall ohne zugehörige Rechtsgrundlage! [1, 2] - andererseits ist eine zielgerichtete Überwachung einzelner Geräte mittels IMSI-Catcher überhaupt nicht möglich, da sich der Catcher gegenüber den Endgeräten als Funkzelle ausgibt. Somit bauen alle alle im Umkreis aktiven Geräte eine Verbindung zum IMSI-Catcher auf, um sich in das Mobilnetz einzuwählen, und werden so einer Überwachung ohne Rechtsgrundlage ausgesetzt [3].

Empfehlung: Die Maßnahme verfehlt ihr Ziel und ist als nicht verhältnismäßig einzustufen. Wir empfehlen die ersatzlose Streichung aus dem Entwurf.

[1] Stefan Krempl: *26C3: GSM-Hacken leicht gemacht*. In: *Heise News*. Heise Zeitschriften Verlag.
[2] GSM: SRSLY?, Talk von Chris Paget und Karsten Nohl am 26. Chaos Communication Congress. abrufbar unter https://media.ccc.de/v/26c3-3654-en-gsm_srsly
[3] https://de.wikipedia.org/wiki/IMSI-Catcher#Funktionsweise

Überwachung von verschlüsselten Nachrichten, § 135a (1)

Um eine Überwachungssoftware auf einem Computersystem zu installieren, müssen etwaige Sicherheitsvorkehrungen am Computersystem überwunden werden, wodurch auch Zugriff auf persönliche Daten erlangt wird. Das ist ein massiver Eingriff in die Privatsphäre (weit über die Überwachung von Nachrichten hinausgehend) und des weiteren eine staatliche Maßnahme, die im wesentlichen die Installation eines Root-Kits bedeuten würde. Nur mit einem Root-Kit wäre es möglich, die Installation der Überwachungssoftware für die Benutzer_innen unsichtbar zu gestalten. Mit einem installierten Root-Kit werden allerdings alle Ermittlungsergebnisse unbrauchbar, da

mit einem Root-Kit beliebige Daten am Computersystem hinterlegt oder manipuliert werden können.

Für die Anschaffung von Software/Hardware, die eine Umgehung von Sicherheitsmaßnahmen möglich macht, wäre unter Umständen eine Kooperation mit Sicherheitsfirmen notwendig, die aktiv nach Sicherheitslücken suchen und diese gegen Geld verkaufen. Diese unethische Praxis sollte vom Staat Österreich keinesfalls unterstützt werden - solche Firmen machen *alle* Benutzer_innen von Computersystemen weniger sicher. Da Sicherheitslücken zwischendurch immer wieder entdeckt und repariert werden, müsste auch regelmäßig Geld in fragwürdige Firmen investiert werden.

Die Geheimhaltung von für Überwachungssoftware notwendigen Sicherheitslücken stellt eine massive Gefahr für öffentliche Infrastruktur dar, wie der Ausbruch der Ransomware Wanna Cry dieses Jahr gezeigt hat. [1]

Für die Installation der Überwachungssoftware reicht der Verdacht aus, dass eine tatverdächtige Person ein bestimmtes Computersystem benutzen oder mit ihm eine Verbindung aufbauen würde. Das ist sehr allgemein gefasst und würde auch Internet-Cafés, Internet-Räume an der Uni, Computersysteme von Freund_innen und Verwandten betreffen (da mit diesen eine Verbindung aufgebaut werden könnte). Laut den Definitionen in § 143 (3) umfasst diese Überwachung nicht nur Nachrichten und verschlüsselte Nachrichten, sondern auch "Informationen, die über ein Kommunikationsnetz (§ 3 Z 11 TKG) oder einen Dienst der Informationsgesellschaft (§ 1 Abs. 1 Z 2 des Notifikationsgesetzes) gesendet, übermittelt oder empfangen werden". Dies kann Postings auf sozialen Medien (Facebook, Twitter, Instagram) genauso umfassen wie Login-Daten.

Unseres Erachtens bedeuten diese Definitionen und Voraussetzungen bedeuten eine immens breite Anwendbarkeit und sind zu weit interpretierbar.

Empfehlung: Die vorgeschlagene Maßnahme greift unverhältnismäßig tief in die Privatsphäre der Betroffenen ein und würde eine Zusammenarbeit mit unethisch agierenden Unternehmen fördern. Da die Überwachung von persönlichen Nachrichten grundsätzlich problematisch ist, schlagen wir die ersatzlose Streichung vor.

[1] http://www.crypto.com/blog/between_immediately_and_never

Beschlagnahme von Briefen, § 135 (1)

Die Streichung der Einschränkung " *[...] und sich der Beschuldigte wegen einer solchen Tat in Haft befindet oder seine Vorführung oder Festnahme deswegen angeordnet wurde*" bedeutet eine faktische Aufhebung des Briefgeheimnisses in

Österreich. Das weckt in uns Erinnerungen an den Metternich'schen Spitzelstaat, die DDR und andere autoritäre Regime.

Das in der Folgeabschätzung formulierte Ziel der "Wahrung grundrechtlicher Standards" kann hier nur als verfehlt angesehen werden.

Empfehlung: Die vorgeschlagene Maßnahme bietet zu viel Missbrauchspotential (siehe auch unsere Stellungnahme zur Novelle des SPG [1]) und ist deshalb ersatzlos aus dem Entwurf zu streichen.

[1] https://www.fsinf.at/stellungnahme-zum-%C3%BCberwachungspaket-ministerialentwurf-326me

Optische und akustische Überwachung von Personen, § 136 (1a)

Die Einführung der "optischen und akustischen Überwachung von Personen" in Fahrzeugen ist insgesamt unübersichtlich, schwammig und verwirrend gestaltet. Statt ordentliche Voraussetzungen zu definieren wird auf einen bereits vorhandenen Paragraphen, der aber auf einen anderen Einsatzbereich hat, verwiesen. Im Informatik-Bereich nennt sich so etwas "dangling pointer" [1]. Der Begriff "Fahrzeug" ist viel zu weit dehnbar, als dass er hier haltbar wäre - gelten z.B. öffentliche Verkehrsmittel ebenfalls als Fahrzeuge?

Abgesehen von diesen unsauberen Definitionen wurden außerdem Ankündigungen bezüglich der Voraussetzungen nicht eingehalten und der Rahmen der Voraussetzungen stark aufgeweicht (Strafandrohung von 1 Jahr statt 3 Jahren).

Aufgrund unsauberer Definitionen und zu stark aufgeweichter Voraussetzungen beinhaltet diese Maßnahme ein hohes Missbrauchspotential sowie rechtliche Unsicherheiten.

Empfehlung: Wir empfehlen die ersatzlose Streichung aus dem Entwurf.

[1] https://en.wikipedia.org/wiki/Dangling_pointer

Fachschaft Informatik

Technische Universität Wien