# Centre for Informatics and Society (CIS), TU Wien

## Stellungnahme im Begutachtungsverfahren zum Überwachungspaket (325/ME, 326/ME)

Das Centre for Informatics and Society (CIS) der Fakultät für Informatik an der Technischen Universität Wien nimmt zu den vorliegenden Ministerialentwürfen 325/ME und 326/ME im Rahmen des sogenannten Überwachungspakets Stellung und äußert schwerwiegende Bedenken.

Das CIS beschränkt sich in seiner Stellungnahme aufgrund des Ausmaßes der vorgeschlagenen Änderungen auf die wichtigsten Punkte und gibt eine Einschätzung aus überwiegend technischer Sicht ab. Dies ist keinesfalls als Zustimmung zu den nicht erwähnten Punkten zu verstehen.

Viele der im Vorschlag erwähnten Maßnahmen sind aus technischer Sicht kaum oder nicht im geforderten Ausmaß implementierbar; andere wiederum haben weitreichendere Auswirkungen auf die Sicherheit von Computersystemen als im Entwurf berücksichtigt.

Eine staatliche Sicherheitsstrategie muss aus Sicht des CIS in einem faktenbasierten Prozess unter Zuzug von Expertisen nicht nur aus juristischer, sondern auch technischer und gesamtgesellschaftlicher Sicht entworfen werden. Das CIS ist zur Mitwirkung an einem solchen Prozess gerne bereit, eine Expertise aus technischer Sicht abzugeben.

Konkret bezieht das CIS Stellung zu folgenden Punkten:

1. Die in § 135a Abs. 3 StPO-E angeführte „Überwindung von spezifischen Sicherheitsvorkehrungen“ setzt bei realistischer Betrachtung voraus, dass zur Einbringung der im Gesetzesentwurf beschriebenen Software Sicherheitsschwachstellen am Zielsystem ausgenutzt werden müssen. Dies gilt insbesondere für die mit diesem Entwurf ermöglichte »remote installation«. Damit bringt sich der Staat in mehrere Interessenskonflikte.

    1. Der Staat muss als Folge dieses Gesetzes an der Geheimhaltung der Sicherheits-Schwachstellen in Computersystemen interessiert sein, während er gleichzeitig, beispielsweise in der „Österreichischen Strategie für Cyber Sicherheit“, explizit ein gegenteiliges Interesse verfolgt.
    2. Während davon auszugehen ist, dass selbst aktuell gehaltene und gut geschützte technische Systeme Schwachstellen besitzen, werden solche Schwachstellen üblicherweise über einen eigenen Markt vertrieben bzw. erworben. Ein im Rahmen der Anwendung dieses Gesetzes voraussichtlich notwendiger Erwerb von sogenannten „Zero-Day Exploits“ – also Fehler in Computersystemen, für die es noch keine Behebung gibt – auf einem solchen Markt bedeutet, dass nicht gesetzkonforme Aktivitäten mit Steuergeldern direkt finanziert werden. Zum Schutz dieser Investition muss der Staat wiederum ein Interesse daran entwickeln, dass eine ausgenutzte Sicherheitslücke weder bekannt noch vom Hersteller behoben wird. Damit wird ein Risiko für alle Betreiber und Nutzer eines betroffenen Systems geschaffen.

    Der im zweiten Punkt beschriebene Interessenkonflikt konnte in jüngster Vergangenheit an einer sich rasant ausbreitenden Schadsoftware beobachtet werden. Die Erpressungs-Software, die unter dem Namen »WannaCry« (auch: »WannaCrypt«) bekannt wurde, ist im Wesentlichen eine „scharfgemachte“ Version einer Software, die von der NSA entwickelt wurde, um in Computersysteme eindringen zu können. Dafür wurde eine Schwachstelle in Microsoft Windows über 5 Jahre nicht kommuniziert.

Es entsteht damit also eine Situation, in der der Staat, im Namen der Sicherheit, die Sicherheit seiner Bürger_innen gegenüber cyberkriminellen Angriffen de facto verringert.

Zusätzlich schreibt § 135a Abs. 2 Z 1 StPO-E vor, dass die Software nach Beendigung der Ermittlungsmaßnahme ohne dauerhafte Schädigung oder Beeinträchtigung des Computersystems entfernt oder funktionsuntüchtig gemacht werden kann. Aus unserer Sicht ist dies in der Praxis unmöglich. Die Installation einer solchen Software ist in Systemen mit heute üblicher technischer Komplexität kaum reversibel verwirklichbar.

2. Die im § 135 Abs. 2a StPO-E angeführte „Lokalisierung einer technischen Einrichtung“ unter Bezugnahme auf die internationale IMSI-Kennnummer unter Verwendung eines sogenannten IMSI-Catchers ist eine technische Maßnahme, welche weit über die bloße Lokalisierung der entsprechenden technischen Einrichtung hinausgeht; diese ermöglicht unter anderem das Abhören von Gesprächen ohne weitere Rechtsgrundlage. Darüber hinaus ist eine zielgerichtete Überwachung einzelner technischer Einrichtungen mittels IMSI-Catcher nicht möglich, da sich das Gerät gegenüber anderen Endgeräten als Funkzelle ausgibt und somit alle im Umkreis verfügbaren technischen Einrichtungen über den IMSI-Catcher geroutet werden; diese anderen Endgeräte sind so einer Überwachung ohne Rechtsgrundlage ausgesetzt.

   Abhören von Mobiltelefonen ist schon seit langem über die Kooperation mit Mobilfunkanbietern möglich; dieser Ansatz ist für den Überwachten - im Gegensatz zur Verwendung von IMSI-Catchern - nicht erkennbar und daher für die Behörde von Vorteil. Es ist nicht klar, welche Vorteile durch den Einsatz von IMSI-Catchern erwartet werden.

3. Die im § 17, Abs. 1a TKG-E vorgeschlagene Befugnis für Anbieter von Internetzugangsdiensten (Provider), Verkehrsmanagementmaßnahmen zu etablieren, stellen einen massiven Eingriff in die Netzneutralität dar. Sie ermöglichen den Anbietern auch die kommerzielle Verwertung solcher Maßnahmen unter dem Deckmantel der Vermeidung von strafrechtlich relevanten Handlungen. Aus technischer Sicht sind die derzeit üblichen Maßnahmen wie DNS- oder IP-Sperren leicht zu umgehen, bergen aber gleichzeitig das Potential, unbeteiligte Dritte zu treffen (deren Inhalte etwa unter derselben IP-Adresse abzurufen sind). Somit sind Netzsperren keineswegs ein probates Mittel zur Vermeidung von strafrechtlich relevanten Handlungen.

Für das CIS Board of Directors

Ao. Prof. Dipl.-Ing. Dr. techn. Hilda Tellioglu
(Vorsitzende des Boards)

Wien, am 18.08.2017

Rückfragen an
cis@cisvienna.com