Stellungnahme der Fakultät für Informatik zum geplanten Sicherheitspaket

Der Fakultätsrat der Fakultät für Informatik an der Technischen Universität Wien nimmt zum geplanten Sicherheitspaket der österreichischen Bundesregierung Stellung und äußert schwerwiegende Bedenken.

Die Fakultät beschränkt sich in ihrer 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 der Fakultät in einem faktenbasierten Prozess unter Zuzug von Expertisen nicht nur aus juristischer, sondern auch technischer und gesamtgesellschaftlicher Sicht entworfen werden. Die Fakultät ist zur Mitwirkung an einem solchen Prozess gerne bereit, eine Expertise aus technischer Sicht abzugeben.

Konkret bezieht der Fakultätsrat 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.

    a) 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.
    b) 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.

Die Einschränkungen in § 134 Abs. 3 der Überwachung auf *„Nachrichten und Informationen, die von einer natürlichen Person […] gesendet, übermittelt oder empfangen werden“* ist ebenfalls problematisch. Eine klare Zuordnung, ob Datentransfer im Sinne von *„Nachrichten und Informationen“* durch einen automatisierten Softwareprozess oder durch eine natürliche Person initiiert wurden, ist technisch nicht immer eindeutig möglich.

Zusätzlich schreiben §§ 135a Abs. 2 Z 1 und 145 Abs. 4 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 und Mobilität kaum garantiert reversibel verwirklichbar.

2) Die im § 135 Abs. 2a StPO-E angeführte *„Lokalisierung einer technischen Einrichtung*“ unter Bezugnahme auf die *„zur internationalen Kennung des Benutzers dienenden Nummer (IMSI)*“ ohne Mitwirkung von Mobilfunk- oder anderer Anbieter ist nur durch die Verwendung eines sogenannten IMSI-Catchers realisierbar. Dies jedoch wäre eine technische Maßnahme, welche weit über die bloße Lokalisierung der entsprechenden technischen Einrichtung hinausgeht und ermöglichte 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.

Für die Fakultät für Informatik der TU Wien

Univ.Prof. Dr. techn. Hannes Werthner — Univ.Prof. Dr.techn. Reinhard Pichler

(Dekan der Fakultät) — (Vorsitzender des Fakultätsrats)

Wien, am 7.3.2018