Ulrich Lintl

14.08.2017

Ulrich Lintl nimmt zu dem Entwurf wie folgt Stellung:

Stellungnahme im Begutachtungsverfahren zum Ministerialentwurf des Justizministeriums, Strafprozessrechtsänderungsgesetz 2017 (325/ME)

Der “Bundestrojaner” an sich ist schon in mehrfacher Hinsicht ein Problem: Es ist eine Software, die Sicherheits-Lücken auf Computern ausnutzt, um Daten auszulesen – und stellt somit einen schweren Eingriff sowohl in die Privatsphäre der Menschen dar, als auch in deren IT-Sicherheit. Es ist das eine Methode, die meist von Cyber-Kriminellen durchgeführt wird.

Er ist – wie u.a. von Epicenter-Works, richtig analysiert, auch sehr unzuverlässig – jedenfalls bei Menschen, die sich mit IT-auskennen: Durch Anti-Malware-Programme können Trojaner erkannt und eliminiert werden. Dazu kommt noch die Möglichkeit, dass Überwachte bei Erkennen von Malware den Überwachern bewusst falsche Daten liefern.

Zusätzlich besteht auch noch die – bereits auf dramatische Art eingetretene – Gefahr, dass von Staaten entwickelte oder verwendete Malware in die falschen Hände gerät und dann zur Überwachung oder sogar Zerstörung fremder Computer-Anlagen führt. Eines der bekanntesten Beispiel dafür ist der Krypto-Trojaner “Wannacry”, der ja erst vor wenigen Monaten in zahlreichen Ländern Krankenhäuser, Unternehmen und sogar Behörden befallen hat.

Und um überhaupt einen Bundestrojaner oder andere Malware seitens Behörden “erfolgreich” einsetzen zu können, ist es notwendig, dass Sicherheitslücken offen bleiben. Dadurch und zusätzlich durch die staatliche Malware selbst werden Unternehmen, NGOs und Einzelpersonen seitens des Staates erheblichen Gefahren ausgesetzt. Die IT ist in unserem Leben so derartig wichtig, dass das Einzelne, Gruppen aber auch den ganzen Staat schwer treffen kann.

Der Staat hat ja auch eine Schutz-Funktion gegenüber seinen Bürgern und aus meiner Sicht auch gegenüber Unternehmen. Deshalb haben Behörden in meinen Augen sogar die Verpflichtung, bekannte Sicherheitslücken unverzüglich an die entsprechenden Software-Hersteller zu melden, damit diese möglich rasch auf Sicherheitslücken reagieren zu können.

Damit im Zusammenhang: Verschlüsselte Kommunikation ist nicht nur zur Wahrung der Privatsphäre der Nutzer wichtig, sondern auch zu deren eigener und der Sicherheit der von ihnen vertretenen Firmen / Organisationen. Denn Daten werden heute schon als “Gold des 21. Jahrhunderts” bezeichnet. Mit ihnen ist oft auch ein immenser finanzieller Wert verbunden. Daher haben Kriminelle, Mitbewerber und fremde Geheimdienste immer öfter großes Interesse an diesen Daten – und unverschlüsselt sind diese natürlich besonders einfach abzugreifen.

Auch wenn derartige Überwachungsmaßnahmen für mich alleine schon aus prinzipiellen Gründen kategorisch abzulehnen sind, so kommt verschärfend hinzu, dass zahlreiche Experten die schwammige Formulierung des Geltungsbereichs des Gesetzes kritisieren.

Auch staatliche “Man-in-the-Middle” Attacken egal ob bei Datenverbindungen im Internet oder Telefon-Gesprächen, sind Methoden, welche ebenfalls primär von Cyber-Kriminellen angewandt werden, und von denen unser Rechtsstaat die Finger lassen sollte.

Das geplante Abhören von Gesprächen in Autos ist ein weiterer Puzzle-Stein im Aufbau eines Überwachungsstaates.

Die Maßnahmen in diesem Gesetzesentwurf stellen für mich einen schweren Bruch der Privatsphäre dar und sind rechtlich bedenklich bis unzulässig. Alles zusammen ist das so ziemlich das Gegenteil eines freiheitlich-demokratischen Staates, es stellt gleich mehrere Schritte Richtung Diktatur dar.

Ich hoffe, dass dies auch die Parlamentarier erkennen und statt diesem Gesetz nur Maßnahmen befürworten, die im Geiste unserer demokratischen Republik stehen.

Mit freundlichen Grüßen, Ulrich Lintl