

Dr. Christoph Mayr

05.08.2017

Dr. Christoph Mayr nimmt zu dem Entwurf wie folgt Stellung:

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

Bundestrojaner

Eine Legalisierung einer staatlichen Spionagesoftware, eines sogenannten Bundestrojaners, in § 135a StPO-E zur Überwachung verschlüsselter Nachrichtenübertragung ist nicht anzuraten.

Durch die Einführung staatlicher Spionagesoftware investiert der Staat gezielt in kriminelle Programme und die Unsicherheit der häufigsten Betriebssysteme. Um einen Bundestrojaner auf dem Zielgerät zu installieren, müssen Sicherheitslücken geheim- und damit offengehalten werden, da eine unbemerkte Installation sonst nicht zu bewerkstelligen ist. Die desaströsen Folgen von staatlicher Spionagesoftware wurden eindrücklich mit dem weltweiten Angriff des "WannaCry"-Erpressungstrojaners demonstriert. Diese global agierende Schadsoftware, die Krankenhäuser, Bahnhöfe und tausende Unternehmen lahmgelegt hat, wurde erst dadurch ermöglicht, dass die NSA eine ihr bekannte Sicherheitslücke in Microsoft Windows für ihre Spionagesoftware geheim gehalten hatte, anstatt durch Meldung an Microsoft für deren Behebung zu sorgen [1]. Derartige Sicherheitslücken werden zumeist für viel Geld auf zweifelhaften Märkten gehandelt. Einerseits werden diese Märkte bei Ankauf der Lücken durch österreichische Steuergelder finanziert, andererseits wird die gesamte IT-Sicherheit unterminiert, da die Bundesregierung Interesse daran haben muss, dass (durch die Überwachungssoftware ausgenutzte) kritische Sicherheitslücken in den gängigsten Betriebssystemen nicht geschlossen werden, um die Funktionalität dieser Software zu gewährleisten.

Insbesondere durch die Ermöglichung der Ferninstallation der Software im Entwurf wird in den Fortbestand der gefährlichsten Art von Sicherheitslücken

für die Ferninfektion eines Rechners investiert. Somit ist jeder Mensch, der einen Personal-Computer, ein Smartphone, ein Tablet oder eine Spielekonsole verwendet, von dem in Begutachtung gegebenen Gesetz unmittelbar betroffen [2]. Diese und andere Argumente haben 2016 zu einer Kehrtwende von Justizminister Brandstetter geführt, als dieser den bislang letzten Versuch staatliche Spionagesoftware zu legalisieren fallen gelassen hat. [3]

Eine von BMI und BMJ eingesetzte interministerielle Expertenarbeitsgruppe [4] unter der Leitung von Univ.-Prof. Dr. Bernd-Christian Funk hat im Jahr 2008 festgestellt, dass „Online-Durchsuchungen“ von Computersystemen mittels „Trojanern“ nach der österreichischen Rechtsordnung (insb. StPO, SPG und MBG) nicht zulässig sind, da die erforderlichen Ermächtigungen de lege lata nicht vorliegen. Eine Abgrenzung der "Online-Durchsuchung" der Dateien auf dem Computer (Fotos, Tagebücher, etc) von der "Online-Überwachung" der getätigten Kommunikation (WhatsApp, Skype) ist jedoch technisch nicht möglich. Um auch nur einen Bruchteil der gängigsten Messenger erfassen zu können, muss die staatliche Überwachungssoftware einen kompletten Überblick über alle Dateien des Zielsystems haben! Durch die Erläuterungen des Gesetzes wird darüber hinaus klar, dass sogar der "Aufruf von Websites" unter die Überwachung fallen soll!

Die Überprüfung der Software soll laut dem Entwurf durch die Datenschutzbehörde erfolgen. Dies erscheint angesichts der Tatsache, dass der Datenschutzbehörde kein einziger Techniker angehört, und diese seit Jahren chronisch unterfinanziert ist, wie das bewusste Ausschalten von Kontrolle, was zum nächsten Überwachungsskandal geradezu einlädt.

Aus technischer Sicht kommen berechtigte Zweifel auf, ob der Einsatz der geplanten Überwachungssoftware überhaupt geeignet ist, zu einer Bekämpfung von Straftaten beizutragen. Der aktuelle Stand der Technik lässt eine treffsichere, schadlose, unbemerkte und zuverlässige Anwendung gar nicht mit ausreichender Sicherheit zu. Technische Zwischenfälle im Rahmen des Einsatzes könnten leicht zu einem Fehlschlagen oder Bekanntwerden der Ermittlungen führen.

Einerseits werden auch nur halbwegs technisch versierte Benutzer des kompromittierten Computersystems die aufgespielte Schadsoftware erkennen und ihr Verhalten dementsprechend ändern. Andererseits ist es sehr wahrscheinlich, dass der Einsatz der Überwachungssoftware durch Anti-Viren-Software erkannt und unterdrückt wird. Kaspersky Lab gab in einer Stellungnahme bekannt, dass, wenn ein Staatstrojaner von einer Antivirus-Software erkannt wird, dieser daran gehindert wird, Überwachungsdaten nach außen zu leiten. Ein erhöhtes ausgehendes Datenaufkommen oder eine unerklärt erhöhte CPU-Leistung kann auch von technisch nicht versierten Benutzern leicht selbst erkannt werden. Sollte der Betroffene die Überwachungssoftware entdecken, könnte er diese missbrauchen und den Ermittlern falsche Ergebnisse liefern (gezielte Beweismanipulation, Legen einer falschen Fährte). Durch diese falschen Ergebnisse wäre die Ermittlung im besten Fall nutzlos. Noch bedenklicher erscheint aber die Tatsache, dass fehlgeleitete Ermittlungen dazu führen können, dass Kriminelle vom tatsächlich geplanten Vorhaben ablenken und dieses in Ruhe verwirklichen

können. Der Einsatz der Überwachungssoftware selbst wird somit zu einer erheblichen Gefahr für die öffentliche Sicherheit.

Abgesehen davon wird durch den Einsatz der besagten Software an sich ein enormes Risiko für die gesamte Bevölkerung geschaffen! Ist eine solche Software erst einmal im Umlauf, so kann sie sich verselbständigen, missbraucht werden usw, und in Windeseile bei Millionen von Nutzerinnen und Nutzern enormen Schaden anrichten.

Die Überwachung betrifft nicht nur denjenigen, für den diese Überwachung angeordnet wurde, sondern auch alle anderen, die in irgendeiner Weise mit der überwachten Person zu tun haben; und dies in ausgedehntester Weise. Schließlich betrifft die Überwachung auch nicht nur die direkte Kommunikation, sondern zwangsläufig auch den Aufruf von Websites, alle Dateien des Geräts und etwa Inhalte in einer Cloud, an der zB mehrere Menschen gemeinsam arbeiten (siehe oben).

Aus all diesen Gründen bedeutet die geplante Novelle einen massiven, unverhältnismäßigen und verfassungswidrigen Eingriff in die Grundrechte der gesamten Bevölkerung, die elektronische Geräte nutzt.

IMSI-Catcher

Eine Ausweitung der Verwendung eines IMSI-Catchers in § 135 Abs. 2a StPO-E ist nicht anzuraten.

IMSI-Catcher sind eine technische Einrichtung, die nicht nur, wie in der Definition unter § 134 Z 2a StPO-E erwähnt, für die Ortung von Mobiltelefonen genutzt werden kann, sondern auch Kommunikationsinhalte überwachen könnte. Dabei wird der so genannte IMSI-Catcher genutzt, um ein Mobilfunknetz zu simulieren, in das sich das entsprechende Mobiltelefon einwählt und darüber mit dem echten Provider kommuniziert (Man-in-the-Middle). Damit erhält der Betreiber des IMSI-Catchers nicht nur Zugriff auf die entsprechenden Standortdaten, sondern eben auch auf die übertragenen Nachrichten, sodass es sich um eine verfassungswidrige Regelung handelt.

Lauschangriff im Auto

Ein großer Lauschangriff im Auto, also die akustische Überwachung von Personen in Fahrzeugen nach § 136 Abs. 1a StPO-E, ist nicht anzuraten.

Im Entwurf wird vorgeschlagen, dass künftig der große Lauschangriff an deutlich geringere Beschränkungen geknüpft sein soll, als bisher, sofern das Abhören in einem Fahrzeug stattfindet. Der große Lauschangriff, eine der schwersten Überwachungsmaßnahmen, die die StPO zur Verfügung stellt, ist bisher nur zulässig für Straftaten, die mit mehr als zehn Jahren Freiheitsstrafe bedroht sind. Nach dem Entwurf soll nun auch schon bei einer Straftat, die mit einer Freiheitsstrafe von mehr als einem Jahr bedroht ist, eine Überwachung im Auto stattfinden. Dies stellt einen unverhältnismäßigen Eingriff in die Grundrechte dar. Die Beschränkung auf Fahrzeuge erscheint hinsichtlich des Grundrechtseingriffs willkürlich, denn Gespräche in einem privaten, geschlossenen Fahrzeug sind nicht weniger schutzwürdig als Gespräche in einer privaten Wohnung.

[1] <http://www.spiegel.de/netzwelt/web/wannacry-die-lehren-aus-dem-cyberangriff-a-1147589.html>

[2] https://epicenter.works/sites/default/files/epicenter_works_1pager_-_bundestrojaner.pdf

[3] <https://epicenter.works/thema/bundestrojaner>

[4] https://epicenter.works/sites/default/files/1pager-legalitaet_bundestrojaner.pdf