

René Mayrhofer

27.07.2017

René Mayrhofer nimmt zu dem Entwurf wie folgt Stellung:

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

Bundestrojaner

Ich bin gegen die Legalisierung einer staatlichen Spionagesoftware, einem sogenannten Bundestrojaner, in § 135a StPO-E zur Überwachung verschlüsselter Nachrichtenübertragung.

Durch die Einführung staatlicher Spionagesoftware investiert der Staat gezielt in 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 Firmen 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.

****** Ergänzung ****** Der Großteil aller IT-Security-Experten weltweit ist sich einig, dass die Veröffentlichung von Sicherheitslücken mit dem Ziel der schnellen Behebung die einzig taugliche Variante zur besseren Absicherung

von IT-Systemen ist. Die Hoffnung, gefundene Lücken geheim halten oder das Wissen darüber in kleinen Kreisen halten zu können, hat sich in den letzten Jahren mehrfach als falsch herausgestellt, am prominentesten durch die Veröffentlichungen von Edward Snowden oder die jüngsten durch die "ShadowBrokers" Gruppe.

Jede Organisation, die sicherheitskritische Fehler in relevanter Software findet und *nicht* zur Behebung an den Hersteller/Autor meldet, zeichnet sich damit direkt für die dadurch entstehenden Risiken und Schäden verantwortlich. Es ist darauf hinzuweisen, dass die Abhängigkeit der Zivilgesellschaft von IT-Systemen in den nächsten Jahren noch stärker steigen wird. Über Sicherheitslücken in verbreiteten Betriebssystemen wie Android, iOS, Windows, MacOS und anderen werden nicht nur die Endgeräte von Benutzern, sondern direkt oder indirekt auch Systeme der kritischen Infrastruktur angreifbar sein. Dies wird auch die Strom- und Wasserversorgung, elektronische Bezahlssysteme oder eGovernment-Anwendungen betreffen. Sollte der Staat Österreich durch geheim gehaltene Sicherheitslücken dazu beitragen, dass diese durch Dritte ausgenutzt werden, ist der Staat für die Kollateralschäden in die Verantwortung zu ziehen - insbesondere diejenigen Entscheidungsträger, die den Einsatz solcher Lücken angeordnet bzw. genehmigt haben, anstelle zur Verbesserung der Sicherheit der kritischen Infrastruktur beizutragen. Die Kernaufgabe des Staates, für die Sicherheit seine Bürger zu sorgen, wird durch das Horten von Sicherheitslücken konterkariert.

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]

****** Ergänzung ****** In diesem Punkt erlaube ich mir eine Ergänzung aufbauend auf meiner Erfahrung als Leiter einer Forschungsgruppe zur Sicherheit mobiler Systeme (Josef Ressel Zentrum "User-friendly Secure Mobile Environments") in den letzten 5 Jahren und insgesamt etwa 10-jähriger Detailerfahrung mit Android im Speziellen.

Es ist darauf hinzuweisen, dass aktuelle sowie derzeit entwickelte neue Sicherheitsmaßnahmen in den am weitesten verbreiteten mobilen Betriebssystemen Android und iOS die Ausnützung von etwaigen Sicherheitslücken zur Ferninstallation von Software massiv erschweren werden. Für die im Gesetz angedachte Funktionalität zur Überwachung von Messenger-Diensten wie WhatsApp müsste ein solche Trojaner zudem Berechtigungen besitzen, welche deutlich über die einer normalen App hinausgehen. Um in die internen Funktionen anderer Apps eingreifen zu können, d.h. Nachrichten/Inhalte vor deren Verschlüsselung bzw. nach deren Entschlüsselung abzufangen, müsste ein solcher Trojaner in den aktuellen Sicherheitsarchitekturen von Android und iOS über Systemrechte verfügen.

Das entspricht einem Jailbreak für iOS bzw. Rooting unter Android. Mit aktuellen Geräten ist davon auszugehen, dass nur mehr eine lange Kette mehrerer verschiedener Sicherheitslücken die unbemerkte Ferninstallation von Schadsoftware mit Systemrechten erlauben wird, und dass eine solche Modifikation mit höchster Wahrscheinlichkeit zu permanenten Änderungen am System führt. Am Beispiel aktueller Samsung-Telefone würde eine Manipulation auf Systemebene z.B. dazu führen, dass sogenannte eFuses (elektronische Sicherungen) innerhalb des Hauptprozessors durchgebrannt werden. Eine solche Modifikation kann dann prinzipiell nicht mehr rückgängig gemacht werden, sondern erfordert den Austausch der Hauptplatine, um den Urzustand wieder herzustellen. Diese und ähnliche Sicherheitsmaßnahmen bestehen bereits in aktuellen Geräten, und zusätzliche Maßnahmen werden aktuell entwickelt.

Die Forderung des Gesetzesentwurfs, dass nach einer (unbemerkten) Ferninstallation von Schadsoftware einerseits die Überwachung verschlüsselter Kommunikation möglich sein soll, andererseits dieser Trojaner aber wieder vollständig deinstalliert werden können soll, ist daher technisch unrealistisch. Diese Betrachtung ist unabhängig von meiner oben genannten Ergänzung, dass die Nutzung solcher Sicherheitslücken durch einen Staat ethisch und rechtlich mehr als bedenklich ist.

Aus diesen Gründen ist der aktuelle Gesetzesentwurf fehlgeleitet und muss abgelehnt werden.

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, das legitime Ziel der Bekämpfung und Verfolgung von Terrorismus und (organisierter) schwerer Kriminalität zu verfolgen. 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.

IMSI-Catcher

Ich bin gegen die Ausweitung der Verwendung eines IMSI-Catchers in Österreich in § 135 Abs. 2a StPO-E.

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, wofür es keine Rechtsgrundlage gibt.

Lauschangriff im Auto

Ich bin gegen den großen Lauschangriff im Auto, also die akustische Überwachung von Personen in Fahrzeugen nach § 136 Abs. 1a StPO-E.

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, eines der schwersten Überwachungsmaßnahmen, die die StPO zur Verfügung stellt, ist bisher nur zulässig für Straftaten die mit mehr als zehn Jahren Freiheitsstrafe bedroht sind und soll nun auch schon bei einer Straftat, die mit einer Freiheitsstrafe von mehr als einem Jahr bedroht ist, zur Verfügung stehen. Dies stellt einen nicht zu rechtfertigenden 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