9. August 2016

Stellungnahme zur „Quellen-TKÜ“

nach dem Urteil des Bundesverfassungsgerichts vom 20. April 2016

1 BvR 966/09

Constanze Kurz, Linus Neumann,

Frank Rieger, Dirk Engling

1. Einleitung

Eine „Quellen-TKÜ“ (Quellen-Telekommunikationsüberwachung) ist aus technischer Sicht eine Spionagesoftware, die auf einem informationstechnischen System (möglichst) ohne Wissen des Benutzers aufgebracht wird und unbemerkt verdeckte Funktionen ausführt. Zur Infektion des Systems werden vorhandene Schwachstellen benötigt. Nach dieser initialen Infektion ist die Integrität des Systems dauerhaft verletzt.

Für die Ausnutzung von Schwachstellen müssen von staatlicher Seite nicht zwangsläufig sogenannte Zero-Day-Exploits erworben werden, also den Herstellern gängiger Software wie Betriebssystemen, E-Mail-Clients oder Internet-Browsern noch unbekannte und daher noch nicht per Update beseitigte Sicherheitslücken. Diese sind selten und am Markt entsprechend teuer. Im Regelfall genügt es, bekannte, aber vom Besitzer des informationstechnischen Systems nicht durch ein Update korrigierte Schwachstellen auszunutzen.

Die Finanzierung des Erwerbs von Wissen über ausnutzbare Schwachstellen oder von betriebsbereiten Exploits, die Kosten der Spionagesoftware selbst sowie Lizenzgebühren und Kosten der technischen Implementierung und Aktualisierung sind erheblich.[1] Inwieweit und welche Komponenten von staatlichen Behörden derzeit zugekauft werden oder zukünftig erworben werden sollen, ist nicht öffentlich bekannt. Das Bundeskriminalamt (BKA) hat im Rahmen der Anhörung beim Bundesverfassungsgericht zum Bundeskriminalamtgesetz (BKAG) angegeben, eine eigene „Quellen-TKÜ“-Software mit dem Namen „RCIS“ entwickelt zu haben, deren Quellcode dem BKA vorliegen soll. Ob sie nach dem Urteil und der Frist des Gerichts zur Änderung des BKAG

---

[1] In Österreich wird für die „Quellen-TKÜ“ mit jährlichen Kosten von 550.000 Euro bzw. 450.000 Euro kalkuliert: https://www.parlament.gv.at/PAKT/VHG/XXV/ME/ME_00192/fname_521693.pdf, Seite 8.

bis zum 30. Juni 2018 noch nachgebessert werden muss, ist ebenfalls nicht öffentlich bekannt. Die Bundesdatenschutzbeauftragte konnte jedenfalls bislang nach eigenen Angaben keine aktuelle Variante eines Staatstrojaners überprüfen.

Das BKA-Gesetz erlaubt dem BKA zur Abwehr von Gefahren des „internationalen Terrorismus“ mit § 20l die Überwachung der Telekommunikation ohne Wissen des Betroffenen durch Eingriffe „mit technischen Mitteln in vom Betroffenen genutzte informationstechnische Systeme“.

Die „Quellen-TKÜ“ mag zwar dem Namen nach einer normalen TKÜ (Telekommunikationsüberwachung) ähneln, ist aber technisch nicht mit dem Abhören von Kommunikation auf dem Leitungsweg zu vergleichen. Es handelt sich vielmehr um einen heimlichen digitalen Einbruch in ein IT-System. Im BKA-Gesetz werden nicht näher spezifizierte technische Maßnahmen vorgesehen, damit „sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird“. Bei früherer staatlicher Spionagesoftware eines LKAs konnte allerdings keine zuverlässige technische Begrenzung auf bestimmte Überwachungsfunktionen festgestellt werden.[2]

Erfasst die Überwachungssoftware auch andere Informationen als laufende Kommunikation, ist sie als „Online-Durchsuchung“ zu werten. Das BKA-Gesetz erlaubt dem BKA unter engen Voraussetzungen durch § 20k auch diesen verdeckten uneingeschränkten Vollzugriff auf informationstechnische Systeme, ohne eine Einschränkung auf laufende Telekommunikation während der Übertragungsphase.

---

[2] Vgl. Bericht des BayLfD „Prüfbericht Quellen-TKÜ“ vom 30. Juli 2012, https://www.datenschutz-bayern.de/Quellen-TKUE.html, Seite 6.

Nach § 20k Abs. 7 Satz 1 BKAG sollte der Einsatz des Trojaners nur dann unzulässig sein, wenn dabei „allein“ Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden. Das ist wenig lebensnah, denn dass beliebige andere – nicht zur Intimsphäre des Betroffenen gehörende – Daten auf einem informationstechnischen System vorhanden sind, ist im Grunde immer der Fall. Auch für den Trojanereinsatz nach § 20l BKAG war diese Regelung (Abs. 6 Satz 1) vorhanden. Das Urteil zum BKAG führt nun aus, dass der Satz so zu interpretieren ist, „dass eine Kommunikation über Höchstvertrauliches nicht schon deshalb aus dem strikt zu schützenden Kernbereich herausfällt, weil sich in ihr höchstvertrauliche mit alltäglichen Informationen vermischen“.[3]

2. Technische Abgrenzung „Quellen-TKÜ“ und „Online-Durchsuchung“

Funktional ist die „Quellen-TKÜ“ von einer „Online-Durchsuchung“ nur in Hinsicht auf die nach der Infiltration auszuführenden Befehle abzugrenzen. Die Datenzugriffe auf das infizierte System und das Ermitteln der auf dem Gerät installierten Software sind keine bloßen Begleitmaßnahmen, sondern integraler Bestandteil einer heimlichem Ermittlungsmethode, die das Plazieren von Spionagesoftware auf einem System zum Ziel hat, das unter der Herrschaft des Überwachten steht. Sowohl bei der „Quellen-TKÜ“ als auch bei der „Online-Durchsuchung“ müssen während der Infektion Dateien ausgelesen, geändert und geschrieben werden sowie Programme ausgeführt, Sicherheitsmechanismen umgangen und Systembestandteile verändert werden.

---

[3] BVerfG vom 20. April 2016, 1 BvR 966/09, Rn. 222.

Die Beschränkung der Trojanerfunktionen auf die laufenden Telekommunikationsinhaltsdaten zuverlässig und technisch beweisbar umzusetzen, ist praktisch kaum möglich. Zielpersonen können auf eine Vielzahl von Kommunikationskanälen zurückgreifen, darunter E-Mails, Direktnachrichten in sozialen Netzwerken, Instant Messenger, Audio-Dienste etc. Für jede dieser Kommunikationsmöglichkeiten müssten spezifische Lösungen entwickelt, umgesetzt und an das jeweilige System des Betroffenen angepasst werden und dabei ausschließlich Kommunikation erfassen. Insgesamt ist eine Eingrenzung des Funktionsumfangs auf ausschließlich laufende Kommunikation nicht sinnvoll möglich.

Die Herausforderung lässt sich am Beispiel von per Web-Browser aufgerufenen Kommunikationsdiensten wie Web-Mailern oder Social Networks verdeutlichen. Technisch sind diese von der Spionage-Software nicht vom Besuch von klassischen Websites zu unterscheiden. Eine „Quellen-TKÜ“ dürfte zwar das Formulieren einer E-Mail bei einem von vielen weltweit verfügbaren Web-Mailern erfassen, nicht jedoch den Besuch aller anderen im Internet verfügbaren Websites, die vom selben Browser aufgerufen werden. Die Unterscheidung in spezifische Kommunikations- und beliebige andere Websites kann durch eine solche Software nicht treffsicher getroffen werden, ohne dabei „false positives“ oder „false negatives“ zu generieren. Um das Risiko zu minimieren, dass ein Kommunikationsvorgang nicht erfasst wird, wird in der Umsetzung der „Quellen-TKÜ“ das Risiko gleichzeitig maximiert, auch andere Vorgänge zu erfassen. Dabei besteht auch immer das Risiko, den geschützten Kernbereich der privaten Lebensgestaltung zu verletzen.

3. Abgrenzung TKÜ und „Quellen-TKÜ“

Eine „Quellen-TKÜ“ (nach § 20l Abs. 2 BKAG) muss auf die laufende Kommunikation beschränkt werden. Ein laufender Kommunikationsvorgang kann entweder beim Informationsmittler erfasst werden und fällt dann unter Art. 10 Abs. 1 GG oder im Herrschaftsbereich des Kommunizierenden, also direkt am Endgerät. Diese Art der Überwachung von Telekommunikationsdaten am Endgerät ist mit einer hohen Eingriffsintensität und einem direkten Eingriff in das informationstechnische System immer verbunden, denn die Infektion des Computers ist Voraussetzung für das Aufspielen des Trojaners. Dass eine „Quellen-TKÜ“ ausschließlich das Telekommunikationsgeheimnis nach Art. 10 GG beeinträchtigen würde, kann daher nicht überzeugen, da immer auch die Integrität des Zielsystems verletzt wird. Entsprechend wird bei Betroffenen der „Quellen-TKÜ“ in das am 28. Februar 2008 vom Bundesverfassungsgericht etablierte Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme eingegriffen.

Fraglich bleibt, ob beim Einsatz einer Spionagesoftware bei einer „Quellen-TKÜ“ überhaupt von einer Telekommunikationsüberwachung im eigentlichen Sinne gesprochen werden kann. Die Telekommunikation beginnt erst im Moment des Aussendens einer Mitteilung, die „Quellen-TKÜ“ soll jedoch bereits davor aufzeichnen, nämlich beim Erstellen der Nachricht. Übertragen auf den Briefverkehr auf Papier handelt es sich um eine Form der Überwachung, bei der die Inhalte der Briefe und auch bloße Formulierungsversuche beim Absender auf dem Schreibtisch gelesen werden, bevor sie in einem Umschlag gesteckt und in den Briefkasten geworfen oder nachdem sie beim Empfänger geöffnet wurden. Diese Form des Aufzeichnens von Nachrichten ist

deswegen keine Telekommunikationsüberwachung, weil sie gerade unmittelbar vor oder nach und nicht während der Telekommunikation stattfindet.

Festgehaltene Gedanken und Notizen eines Betroffenen, die sein informationstechnisches System nicht verlassen, aber vom Trojaner aufgezeichnet oder gar später ausgewertet werden, sind also keine Kommunikation. Sie mögen zwar für Ermittler von Interesse sein, das rechtfertigt jedoch nicht, sie im Rahmen einer Überwachung zu erfassen. Für die „Quellen-TKÜ“ darf der Datenzugriff auf dem Transportweg erfolgen, ansonsten handelt es sich um eine „Online-Durchsuchung“ und ist auch rechtlich so zu behandeln.

Ebenso verhält es sich beim Protokollieren von verschriftlichten Gedankengängen oder Momentaufnahmen, etwa wenn das Spionageprogramm beim Betroffenen verschiedene Versionen einer E-Mail oder Entwürfe von Texten erfasst, die später verworfen und nicht gesendet oder wieder umformuliert werden. Technisch kann das beispielsweise durch sog. Application-Shots durchgeführt werden, vergleichbar mit dem Abfotographieren eines aktiven Software-Fensters. Ob die dabei festgehaltenen Texte aus einem laufenden Telekommunikationsvorgang stammen oder vor dem Absenden geändert oder gar nicht gesendet werden, ist den Aufnahmen nicht zu entnehmen.

Es ist also nicht nur sicherzustellen, dass der Trojaner nicht auf andere Daten als Telekommunikationsdaten Zugriff nehmen kann, sondern auch, dass Vorbereitungshandlungen, die keine Kommunikation sind, nicht erfasst werden. Generell sind Vorbereitungshandlungen für eine mögliche spätere Kommunikation oder Änderungen an bereits empfangener, früherer Kommunikation für die Spionagesoftware schwer zu trennen von tatsächlich stattfindender Kommunikation, die erfasst werden dürfte. Da der Trojaner immer für einen gewissen Zeitraum auf dem informationstechnischen System plaziert wird, besteht die Gefahr, dauerhaft verschriftlichte Gedanken oder bloße Vor-

bereitungshandlungen von Kommunikation zu erfassen, die aber noch keine Kommunikation sind und vielleicht auch niemals werden.

Die heute typischen Arten von infizierbaren Systemen, die der Gesetzgeber und auch das Bundesverfassungsgericht für die „Quellen-TKÜ“ im Blick hat, sind technische Geräte wie Computer und Mobiltelefone. Darüber hinaus und vor allem zukünftig müssen sehr viel mehr vernetzte Systeme in Betracht gezogen werden, durch die Menschen kommunizieren. Zu denken ist beispielsweise an Kraftfahrzeuge oder Medizinalgeräte, die zur direkten und indirekten Kommunikation genutzt werden und ohne Zweifel informationstechnische Systeme sind. Wer etwa ein elektronisches Hörgerät nutzt, sollte nicht fürchten müssen, eine unfreiwillige Wanze zu tragen.

Angesichts der bereits vorgetragenen Wünsche während der Justizminister-Konferenz, den Einsatz der Staatstrojaner nicht mehr nur gegen „internationalen Terrorismus“ (wie im BKAG vorgesehen), sondern auch bei anderen Straftaten[4] zu ermöglichen, sollte die Art der Geräte, die zur Infektion von Staats wegen gehackt werden dürfen, eng begrenzt werden. Bevor ein Ausweiten der legalen Nutzung von Trojanern durch Ermittlungsbehörden erwogen wird, müssen außerdem vergangene Einsätze evaluiert werden.

[4] Vgl. Beschlussvorschlag der Justizminister-Frühjahrskonferenz 2016, die „Quellen-TKÜ“ soll demnach auch für einfache Strafverfolgung eingesetzt werden. https://netzpolitik.org/2016/fruehjahrskonferenz-justizminister-fordern-ausweitung-von-staatstrojanern-auf-mehr-behoerden-und-mehr-straftaten/#Beschlussvorschlag vom Mai 2016.

4. Risiken der Infiltration

Kritisch ist bei der „Quellen-TKÜ“ die Funktion des Nachladens, die erforderlich sein kann, um bei Änderungen am System seitens des Betroffenen oder bei Updates der jeweiligen Kommunikationssoftware auf dem Zielsystem die Spionagesoftware anzupassen. Durch dieses Nachladen kann aus einer „Quellen-TKÜ“ während des laufendes Einsatzes eine „Online-Durchsuchung“ werden, auch eine Raumüberwachung (und damit ein Eingriff in Art. 13 GG) ist technisch möglich. Das Nachladen kann das zusätzliche Risiko eröffnen, dass auch unberechtigte Dritte eigene Module einschleusen.

Der Chaos Computer Club konnte für den Digitask-Staatstrojaner nachweisen, dass ein Nachladen vorgesehen war. Ob dies im Einsatz auch dazu diente, neue Überwachungsfunktionen auf dem bereits infizierten Computer nachzuladen, konnte durch die statische Analyse der Binaries des Digitask-Trojanern nicht verfiziert oder falsifiziert werden. Um dies aber ausschließen zu können, sollte für den Betroffenen und seinen Verteidiger die Einsichtnahme in den Quellcode des Trojaners sowie in die Protokollierung des Einsatzes gewährleistet werden. „Belastbare und abschließende Aussagen über die programmierten Funktionen und Zugriffsmöglichkeiten der eingesetzten Software“ sind auch für Kontrollbehörden ohne Einsicht in den Quellcode nicht möglich.[5]

Ein weiteres Problem stellt auch die Kontrolle der Qualität offensiver staatlicher Angriffswerkzeuge dar. Schon in den Jahren, als die Ermittlungsbehörden den Digitask-Trojaner im Einsatz hatten, konnte wegen des fehlenden Zugangs zum Quellcode keine sinnvolle Kontrolle der Spionagesoftware erfolgen. Offenkundig wurden aber auch keine

---

[5] Bericht des Bundesdatenschutzbeauftragten über Maßnahmen der Quellen-Telekommunikationsüberwachung, http://www.ccc.de/system/uploads/103/original/Schaar-Bericht.pdf, Seite 4.

Versuche gemacht, die Software zu testen: Die Analyse des Chaos Computer Clubs[6] zeigte, dass Dritte den Staatstrojaner ohne hohen technischen Aufwand aus der Ferne übernehmen konnten, entsprechend waren vor dem Einsatz elementare Sicherheitsvorkehrungen des Staatstrojaners gar nicht oder nicht mit ausreichender Kompetenz geprüft worden. Dazu passt auch, dass die Befehle an den Trojaner unverschlüsselt übertragen wurden. Dass die von dem Betroffenen erlangten Daten über Server in den Vereinigten Staaten zum deutschen Landeskriminalamt gelangten, war ebenso entweder nicht entdeckt oder gar ignoriert worden. Generell ist vor Billiglösungen wie dem rechtswidrigen Digitask-Trojaner zu warnen, dessen handwerkliche Mängel erheblich waren, aber offenkundig niemandem in den einsetzenden Behörden auffielen.

Ein weiteres, seltener beachtetes Risiko beim Einsatz von Staatstrojanern ergibt sich für die Ermittlungsarbeit selbst. Bei klassischen „Großen Lauschangriffen“ verfügen Zielpersonen in der Regeln nicht über professionelles Equipment zum Entdecken der Abhöreinrichtung. Selbst wenn Sie diese zufällig oder nach gezielter Suche entdecken, behindern die Zielpersonen damit auch nur die Ermittlungen gegen sich selbst oder Personen in ihrem Umfeld. Bei Staatstrojanern verhält es sich anders: Aufgrund der permanenten Bedrohung durch Schadsoftware im Alltag verfügen viele Nutzer über Detektions- und Abwehr-Software (sog. „Viren-Scanner“). Deren Detektionsregeln stützen sich teilweise auf Heuristiken, primär jedoch auf bis dato bekannte Schadsoftware. Wird ein Staatstrojaner bei einem Einsatz durch eine Zielperson entdeckt, ist davon auszugehen, dass sämtliche parallele Ermittlungsverfahren binnen kürzester Zeit akut von der Ent-

---

[6] Technische Analyse des CCC zum Staatstrojaner: http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf vom 8. Oktober 2011.

deckung bedroht sind: Sobald weitere Zielpersonen die Schadsoftware-Definitionen aktualisieren, werden sie über die Infektion in Kenntnis gesetzt.

Orientiert man sich an den rechtlichen Schranken für den „Großen Lauschangriff“, so ist nicht nur die Schwelle für das Eindringen in den Kernbereich privater Lebensgestaltung bei der Trojanisierung von informationstechnischen Systemen niedriger. Folgende Analogie zum „Großen Lauschangriff“ vermittelt eine Idee, wie sich die heimliche Infektion eines Computersystems im Vergleich zur „Wanze im Schlafzimmer“ darstellt: Unter rechtlich eng definierten Umständen dürfen Ermittler im Rahmen des „Großen Lauschangriffs“ Abhörwerkzeuge auch im Schlafzimmer verstecken und nach einer Kernbereichsprognose dort Gespräche mithören. Niemand würde aber in der realen Welt auf die Idee kommen, für diesen Zweck, etwa um den Technikeinbau oder -austausch zu vereinfachen, die Haustür des Betroffenen durch eine Attrappe zu ersetzen oder ganz auszubauen. Diese Idee wird für den Einbau der Wanze im Digitalen aber aufgrund der sonst eingeschränkten technischen Machbarkeit vorgesehen.

Generell sollte die Diskussion um Risiken der Infektion von Systemen neben dem Schutz von Höchstpersönlichem der Betroffenen dahingehend erweitert werden, ob die Manipulation durch den Trojaner eine Gefahr für Leib und Leben darstellen kann, abhängig von der Natur der Geräte und von deren Funktion. Gefährdungen können bei informationstechnischen Geräten entstehen, wenn die Infektion mit Spionagesoftware ungewollte Fehlfunktionen auslöst oder Kommunikation unterbindet. Zu denken ist beispielsweise an ein medizinisches Gerät, eine Smart-Watch oder ein Mobiltelefon, das Insulinwerte oder Blutdruck misst und den Patienten selbst oder einen Arzt informiert.

Ein Eingriff durch eine Infektion mit einer Spionagesoftware muss verhältnismäßig sein und darf nicht selbst zu weiteren Gefahren führen.

5. Eignung der „Quellen-TKÜ“ als Ermittlungsmaßnahme

Bei der Bewertung, ob die „Quellen-TKÜ“ ein geeignetes Instrument der Strafverfolgung ist, muss berücksichtigt werden, dass Funktionsbeeinträchtigungen bei den infiltrierten Zielsystemen nicht immer vermieden werden können. Insofern ist die „Quellen-TKÜ“ heikler und auch technisch anspruchsvoller als Telekommunikationsüberwachung auf dem Leitungsweg. Zudem ist eine Kontrolle unabdingbar, um sicherzustellen, auch tatsächlich das anvisierte Zielsystem infiziert zu haben, sofern die Infektion „Remote“ (im Fernzugriff) vorgenommen wurde. Anders als beim Abhören auf dem Leitungsweg muss auch mit hohem technischen Aufwand verhindert werden, dass sich unbefugte Dritte „dranhängen“ und bequem mithorchen.

Überwachung mit einer Spionagesoftware lässt sich technisch nicht auf die bloße Kommunikation beschränken, da das Eindringen in den vernetzten Computer selbst und eine Analyse hier gespeicherter Daten und Programme notwendig ist, ebenso die Steuerung des Trojaners von außen nach erfolgter Infiltration. Insofern ist nicht nur die Telekommunikation, sondern immer auch der Datenbestand des Computers betroffen. Typischerweise sind verschiedene Schutzsysteme zu überwinden, die abhängig von der technischen Versiertheit des Betroffenen auch hohe oder unüberwindbare Hürden darstellen können. Wird wegen dieser Schutzsysteme eine Methode zum Aufbringen des Trojaners verwendet, die physischen Zugriff auf das Gerät[7] erfordert, ergeben sich

[7] Physischer Zugriff zur Infiltration ist bereits angewendet worden, vgl. Bericht des BayLfD „Prüfbericht Quellen-TKÜ“ vom 30. Juli 2012, https://www.datenschutz-bayern.de/Quellen-TKUE.html, S. 59f.

neue Probleme technischer und rechtlicher Art, etwa wenn sich dafür Zutritt zu einer Wohnung verschafft werden müsste.

Es sind keine faktenbasierten Zahlen dazu verfügbar, in welchen Fällen das Aufbringen von Staatstrojanern für den Zweck, nutzerseitige Verschlüsselung zu umgehen, ein geeignetes, geschweige denn notwendiges oder gar unverzichtbares Mittel wäre. Was technisch machbar erscheint, soll zwar legalisiert werden, aber nach Angaben der Bundesregierung führen die Behörden des Bundes keine Statistiken über den Umfang der Konfrontation mit gespeicherten verschlüsselten Inhalten.[8] Auf welche Verschlüsselungstechniken Ermittler tatsächlich in ihrer Arbeit treffen, ist daher nicht dokumentiert. Es existiert nicht einmal eine Größenordnung zur Frage, wie oft und in welchen Fällen eine Trojanisierung technisch sinnvoll wäre, um an anderweitig nicht erlangbare verschlüsselte Inhalte zu kommen.[9] Auch eine Kategorisierung der verwendeten Werkzeuge oder der Art der Verschlüsselung ist damit nicht vorhanden. Jenseits der Verhältnismäßigkeitsfragen und der unabwendbaren Schwierigkeiten und Risiken, die mit einer Infiltration einhergehen, ist also auch die Erforderlichkeit nicht belegt, Kommunikationsinhalte noch vor einer eventuellen Verschlüsselung direkt am Computersystem abzufangen.

Es ist daher grundsätzlich zu überdenken, ob Ermittler für die Strafverfolgung auf Überwachungsmethoden wie die „Quellen-TKÜ“ zurückgreifen dürfen.

---

[8] Siehe Antwort der Bundesregierung, Drucksache 18/7183 http://dip21.bundestag.de/dip21/btd/18/071/1807183.pdf vom 30. Dezember 2015, Seite 5.

[9] Vgl. die bislang bekanntgewordenen Fälle, in denen der Digitask-Trojaner zu Einsatz gekommen war. Mit der Spionagesoftware infiziert wurden die Betreiber einer Online-Apotheke, ein Bodybuilder, der Anabolika verkauft haben soll, und Personen, die des Internetbetrugs oder wegen Drogendelikten verdächtigt wurden.

6. Staatliche Interessenkonflikte

In den letzten Jahren ist international eine verstärkte Verbreitung kommerziell angebotener staatlicher Überwachungstrojaner zu verzeichnen.[10] Diese Entwicklung ist problematisch, da das staatliche Ausnutzen von Schwachstellen einen Interessenkonflikt darstellt. Er besteht vor allem darin, dass aus wirtschaftlichen und Gemeinwohlerwägungen heraus ein hohes staatliches Interesse darin liegt, Computer-Schwachstellen schnell zu schließen, um Wirtschaftsspionage zurückzudrängen und die grauen Märkte, in denen diese Sicherheitslücken gehandelt werden, nicht zusätzlich zu befeuern.

Tritt der Staat als Käufer von Exploits auf, liegt es jedoch in seinem Interesse, die Sicherheitslücke möglichst lange selbst ausnutzen zu können und entsprechend nicht zu schließen. Generell wird der europäische Markt durch das Auftreten staatlicher Behörden als Käufer sowohl für die Verkäufer von ausnutzbaren Sicherheitslücken als auch für die spezialisierten Anbieter von Spionagesoftware attraktiver. Wenn die „Quellen-TKÜ“ und damit der Einbruch in informationstechnische Systeme als Ermittlungsinstrument angestrebt wird, sollte zuvor eine Folgenabschätzung vorgenommen werden, um die Effekte auf diesen Markt abzuschätzen.

---

[10] Vgl.: Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, John Scott-Railton (2013): You Only Click Twice: FinFisher’s Global Proliferation, https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/

7. Fazit

Angesichts der Risiken technischer Art und insbesondere wegen der Gefahren, den geschützten Kernbereich der privaten Lebensgestaltung von Betroffenen zu verletzen, sollten die vom Bundesverfassungsgericht gesetzten Schranken für die „Online-Durchsuchung“ vollumfänglich auch für die „Quellen-TKÜ“ gelten.

Der konkreten Gefährdung des hohen gesellschaftlichen Gutes der Integrität von Millionen von informationstechnischen Systemen, deren Sicherheitslücken nicht ausgenutzt, sondern geschlossen werden sollten, steht mit der „Quellen-TKÜ“ ein Werkzeug zweifelhafter Eignung und unklarer Haltbarkeit gegenüber, dessen Einsatz zudem mit hohen Risiken verbunden ist. Sollte weiterhin am Vorhaben festgehalten werden, eine Infektion mit staatlicher Schadsoftware vorzunehmen, muss mindestens die Art der informationstechnischen Systeme, die infiziert werden dürfen, wegen der dargestellten Risiken eng begrenzt werden.