



Chaos Computer Club

Stellungnahme

**zur „Quellen-Telekommunikationsüberwachung“
und „Online-Durchsuchung“
in der Strafprozessordnung**

1 BvR 180/23

Constanze Kurz,
Dirk Engling, Rainer Rehak

9. Juli 2023

Einleitung	3
Vernetzte Gesellschaft	3
Smartphone als Schaltzentrale für alle Lebensbereiche	4
Entwicklungen in der Computersicherheit	5
Werkzeuge der Infiltration und der Datenerhebung	6
Online-Durchsuchung, QuellenTKÜ und QuellenTKÜ+	7
Unsicherheit der Systeme nach der Infektion.....	9
Unzulässige Ausweitung der betroffenen Zielpersonen.....	11
Mangelnde wissenschaftliche Evaluierung.....	12
Fehlendes Risikomanagement für Hacking-Werkzeuge	13
IT-Sicherheitslückenmarkt	13
Kein „Going-dark“ ohne Staatstrojaner.....	15
Fazit.....	16

Einleitung

Mit der Ergänzung der Strafprozessordnung in einem parlamentarischen Schnellverfahren wurde der Einsatz von Staatstrojanern als eine Standard-Maßnahme der strafprozessualen Überwachung auch gegen Alltagskriminalität mit niedriger Eingriffsschwelle definiert. Der dadurch gesetzlich möglich gewordene breite Einsatz von Hacking-Werkzeugen karikiert geradezu das Gefahrenpotential solcher Spionagesoftware.

Diese Stellungnahme des Chaos Computer Clubs (CCC) versucht, die wesentlichen Gefahren zu benennen und technische Änderungen zu erläutern, die den Einsatz von Staatstrojanern in den letzten Jahren prägen. Seit der CCC vor mehr als zehn Jahren deutlich überschießende Funktionalitäten eines praktisch im Einsatz befindlichen deutschen Staatstrojaners nachgewiesen hat, haben sich die Vorgehensweisen zum heimlichen Aufbringen von Spionagesoftware gewandelt. Entsprechend sollten sich auch die rechtlichen Bedingungen diesen tatsächlichen Gegebenheiten anpassen. Der enormen Ausweitung der Einsatzmöglichkeiten von Staatstrojanern sollten Regelungen gegenüberstehen, die das Gefahrenpotential wirksam dämpfen können.

Vernetzte Gesellschaft

Die seit nunmehr fünfzig Jahren zunehmende Digitalisierung der Gesellschaft entwickelt sich aktuell in zwei für die vorliegende Verfassungsbeschwerde relevanten Dimensionen. Einerseits sind elektronische Geräte und Systeme immer dichter an die einzelnen Menschen herangerückt und elementarer Teil der gesamten Lebens- und Arbeitspraxis. Dies bezieht mittlerweile oft weite Teile des Sozialverhaltens mit ein, inklusive des Kernbereichs privater Lebensgestaltung. Für die meisten Menschen ist es nicht mehr möglich, ein normales Leben zu führen, ohne regelmäßig auf informationstechnische Systemen angewiesen zu sein, vom Smartphone bis zum Arbeits-PC.

Andererseits sind diese Systeme auch unverzichtbarer Teil aller gesellschaftlichen Infrastrukturen geworden. Dabei werden die Systeme zunehmend komplexer, der Großteil ist über das Internet miteinander vernetzt. Es ist also auf vielen Ebenen zutreffend, von einer vernetzten Gesellschaft zu sprechen.

Diese Vernetzung hat viele Vorteile, etwa für die weltweite Kommunikation und den freien Wissenstransfer, für eine inklusive und partizipative Demokratie, für optimierte Produktionsprozesse oder für die individuellen Entfaltungschancen der Menschen. Allerdings bedeutet der hohe Grad an technischer Durchdringung und Vernetzung auch eine wachsende gemeinsame Abhängigkeit von diesen Systemen sowie eine gemeinsame Verwundbarkeit. IT-Sicherheit ist daher eine gemeinschaftliche Aufgabe, die durch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme¹ gestärkt wurde.

¹ 1 BvR 370/07, Urteil vom 27. Februar 2008.

Smartphone als Schaltzentrale für alle Lebensbereiche

Seit der Definition des Grundrechts 2008 hat sich die Durchdringung des Alltags der meisten Bundesbürger mit informationstechnischen Systemen weiter intensiviert. Vor fünfzehn Jahren wurden Computer eigens zur Benutzung ein- und grundsätzlich danach wieder ausgeschaltet und Nutzerinnen widmeten sich explizit und bewusst dem Gerät. Die Sensoren der Geräte beschränkten sich auf Webcams und eingebaute Mikrophone.

Heute haben wir es in den meisten Fällen mit untereinander vernetzten multisensorischen Schwärmen von mobilen und stationären Geräten zu tun, die rund um die Uhr eingeschaltet und online sind, automatisiert alle Arten von Informationen – auch intime – aufzeichnen, zusammenführen und in dezentralen Sicherungskopien sowie in persönlichen Clouds verteilen. Zu den lange vertrauten Geräten wie stationären PCs, Notebooks und Tablets gesellt sich inzwischen ein vernetzter Zoo aus Mobiltelefonen, Aktoren und Sensoren der Heimautomatisierung, „smarten“ Haushaltsgeräten und Fernsehern, Fitness- und Aktivitäts-Trackern in Armbanduhrform, „smart Speakern“, Navigationssystemen und „In-car Entertainment“, Hilfsmitteln wie Hörgeräten und „smarten“ Prothesen oder vernetzten Ortungsgeräten wie beispielsweise AirTags oder sogar vernetzten Herzschrittmachern.

Dabei ergibt sich aus der Summe der Aufzeichnungen all dieser vernetzten informationstechnischen Systeme ein deutlich präziseres und auch rückwirkendes Bild über einen Menschen und seine Kommunikations- und Bewegungsabläufe, als dieser es von sich selber gewinnen könnte. Es entsteht ein regelrechtes digitales Dossier über den Menschen, sein Verhalten und auch seine innersten Regungen. Etwaige im Smartphone gespeicherte Gesundheits- und Körperdaten können zusätzlich das Befinden des Menschen detailliert zeigen.

Dies ist teilweise von den Nutzerinnen auch gewollt. Stets ist dabei jedoch die Grundlage, dass die Systeme sicher und die Daten privat sind. Weil die multisensorischen IT-Systeme Menschen so präzise dekonstruieren können, erwarten Nutzerinnen von diesen Systemen auch die vollständige Hoheit über die tiefsten Einblicke in ihr Leben und das der Mitmenschen aus Familie, Freundes- und Kollegenkreis.

Zudem ist die Nutzung verschlüsselter digitaler Dienste – egal ob privat oder beruflich, künstlerisch oder politisch – allgegenwärtig geworden. Noch vor dem Jahr 2016 wäre undenkbar gewesen, dass inzwischen dank Diensten wie „Let’s Encrypt“² faktisch keine Webseiten mehr unverschlüsselt abgerufen werden. Verschlüsselungstechnologien werden nun universell eingesetzt, ihre Anwendung ist von der Ausnahme zur Regel geworden, im Internet insgesamt³ und bei Messengern insbesondere.

² Siehe <https://letsencrypt.org/>

³ Vgl. Encryption and DPI: Current and Future Services Impact, https://www.sandvine.com/hubfs/Sandvine_Redesign_2019/Downloads/Whitepapers/sandvine-wp-encryption-and-dpi.pdf vom 19. Dezember 2017.

Alle verbreiteten Messenger-Dienste wie Facebook Messenger, Signal oder WhatsApp nutzen nunmehr Verschlüsselung und werden auf Smartphones alltäglich privat und beruflich genutzt. Folgt man der Logik des Gesetzgebers bei der „Quellen-TKÜ“ und „Online-Durchsuchung light“ darf das Abhören von laufender verschlüsselter Kommunikation mit Hilfe eines Staatstrojaners nunmehr für einen langen Katalog an Straftaten genutzt werden. Da heute viele Millionen Menschen mittels verschlüsselter Messenger kommunizieren, würde das bedeuten, dass staatliche Schadsoftware in sehr viel mehr Fällen heimlich in den Geräten plaziert werden würde.

Ein weiterer wesentlicher Aspekt der veränderten Nutzung informationstechnischer Systeme ist für viele Menschen die Umwandlung von Smartphones in eine Art Lebensführungszentrale. Es fungiert als Schaltzentrale für alle möglichen Lebensaspekte, ob als elektronische Brieftasche, als digitaler Schlüssel für das Auto, als Haustür-Fernöffner, als zentraler Fahrkartenspeicher, als Mobilitätszentrale, als persönliche Routing- und Navigationsassistentin, als Verwaltungszentrale für Versicherungen und Abonnements oder für den geschäftlichen Zugriff auf besonders abgesicherte Systeme. Viele Services, etwa die Bezahl Dienste von Google, Apple oder bestimmten Banken können gar nur noch via Smartphone verwendet werden.

Auch die aktuellen staatlichen Bestrebungen, hoheitliche Funktionen und Dokumente wie Führerscheine oder Personalausweise aufs Smartphone zu bringen sowie weitere eGovernment-Dienste in der Breite mobil nutzbar zu machen, unterstreichen die zentrale Funktion, die das Smartphone im Leben vieler Menschen längst eingenommen hat. Dabei erzeugt die Nutzung all dieser Dienste weitere Protokoll- und Verhaltensdaten. Das Smartphone ist mittlerweile nicht nur eine Lebensschaltzentrale für viele Menschen geworden, sondern bei geheimem Zugriff darauf auch ein digitaler Universalzugang hinein in all diese Aspekte des Lebens dieser Menschen.

Entwicklungen in der Computersicherheit

Die Hersteller moderner mobiler Betriebssysteme tragen der Informationsexplosion und der oben skizzierten stark geänderten Nutzung Rechnung, indem Geräte und damit die darauf anfallenden Daten deutlich besser gegen unbefugten Zugriff geschützt werden, als noch zu Beginn des mobilen Internetzeitalters. Entscheidungen einiger US-amerikanischer Technologieunternehmen wie Microsoft, Apple und Google im Nachgang der Edward-Snowden-Veröffentlichungen ab Mitte 2013 haben sowohl das Sicherheitsniveau der mobilen Betriebssysteme als auch das der Anwendungen stark angehoben, zumeist in Form verbesserter Verschlüsselungstechnologien und der Einführung strikt genormter Prozesse in der Software-Entwicklung zum Finden, Beheben und Vermeiden von Sicherheitsproblemen.

Die meisten mobilen Systeme sind dadurch inzwischen deutlich besser gegen Angriffe geschützt als stationäre PCs und fungieren zusätzlich zu den oben beschriebenen Nutzungsweisen mit ihren „sicheren Enklaven“ zunehmend als primäre Sicherheitsanker für sicherheitsrelevante Vorgänge wie Überweisungen, Buchungen und Einkäufe aller Art. Mehr noch: Viele Online-Dienste erzwingen inzwischen neben einem Zugangspasswort die sogenannte

Zwei-Faktor-Authentisierung, wobei zusätzlich zum Passwort dann ein Telefon – meistens das Smartphone – für den Empfang von Zugangs-Token verknüpft werden muss, etwa per SMS. Das Smartphone wird also für viele Anwendungen zum digitalen Generalschlüssel des modernen Alltags.

Zum Schutz der Daten und zum Verhindern der schlimmsten Folgen von Software-Fehlern werden von den Betriebssystementwicklern zunehmend rigorosere Werkzeuge der Kompartimentalisierung eingesetzt. Sie sollen den absichtlichen oder irrtümlichen Zugriff einzelner installierter Apps auf bestimmte Sensoren wie Kamera oder Mikrofon, Daten aus anderen Apps oder des Betriebssystems und fortwährender vom Nutzer unbemerkter Aktivität verhindern. Obwohl immer wieder Sicherheitslücken in diesen Schutzmaßnahmen entdeckt und ausgenutzt werden, wurde das allgemeine Sicherheitsniveau der mobilen Endgeräte in den letzten Jahren in Summe substantiell verbessert.

Werkzeuge der Infiltration und der Datenerhebung

Die zunehmend bessere IT-Sicherheit von mobilen Systemen bedeutet, dass heute höhere Hürden übersprungen werden müssen, um ein solches Gerät zu hacken. So gilt, dass im Gegensatz zur vergleichsweise einfachen Installation von Trojanern, beispielsweise auf dem Windows-Betriebssystem durch das unvorsichtige Öffnen eines E-Mail-Anhangs, heutzutage deutlich mehr Aufwand betrieben werden muss. Schon zum unbemerkten Aufbringen einer Überwachungssoftware auf einem aktuellen Mobiltelefon oder Laptop müssen in einer sog. Infektionskette (infection chain) mehrere unterschiedliche unveröffentlichte Sicherheitsprobleme – sogenannte 0-Days – in verschiedenen vertikalen Ebenen mehrerer Softwarekomponenten auf dem Zielrechner ausgenutzt und dabei Schutzmechanismen des Betriebssystems ausgehebelt werden.

Es gibt mehrere Wege, auf das Zielgerät Software einzubringen, grundsätzlich gilt aber: Um verdeckt auf ein modernes informationstechnisches System zugreifen und anschließend Daten auszuleiten zu können, bedarf es im Wesentlichen zweier Schritte. Erstens muss überhaupt der Zugriff auf das Zielsystem durch Überwindung seiner Sicherheitsmechanismen bewerkstelligt werden. Dieser Schritt wird in der Computerwissenschaft als Infiltration oder Infektion des Systems bezeichnet und beinhaltet üblicherweise mehrere weitere Teilschritte.

Veranschaulichen lässt sich eine solche Infektionskette so: Im ersten Schritt kann ein Angreifer beispielsweise an ein iPhone eine Direktnachricht mit einem Bild an die Zielperson senden,⁴ dessen eingebettete strukturierte Formatbeschreibungsdaten die Anzeige-Routine für das entsprechende Bildformat überlisten soll. Die gebrauchsfertig zusammen-geschürte Version einer solchen Software nennt sich „Exploit“, der erfolgreich ausgeführt häufig einen „Dropper“ oder „Installer“ speichert oder nachlädt. Dieser nutzt

⁴ Vgl. Roman Loyola: Report details ‘zero-click’ iOS exploit that can infect an iPhone via iMessage, <https://www.macworld.com/article/1940315/imessage-exploit-ios-15-7-malicious-attachment-zero-click.html> vom 2. Juni 2023.

im weiteren Verlauf der Infektion wiederum Lücken in der Kompartimentalisierung aus und nistet sich selbst oder die in einem letzten Schritt nachgeladene „Payload“ – also den eigentlichen „Trojaner“ – dauerhaft im System ein.

Der zweite Schritt nach erfolgreicher Infiltration besteht im Überwachen, Durchsuchen, Erheben und Ausleiten der gefundenen Daten aus dem Zielsystem, etwa von Bildschirm- oder Kommunikationsinhalten oder gespeicherten Dateien. Dabei werden dann ähnliche oder identische Lücken ausgenutzt, um Dateien zu lesen und zu schreiben, die eigentlich unzugänglich sein sollten, oder beispielsweise um Sensoren gegen den Willen der Nutzerinnen anzuzapfen, verschleierte Netzwerkverbindungen zu etablieren und sich vor Entdeckung und eingebauten Reinigungsfunktionen des Systems zu schützen.

Alle Varianten eines solchen Vorgehens verändern schon durch den ersten Schritt das Zielsystem wesentlich und unterminieren so dauerhaft seine Integrität, unabhängig davon, welche Daten danach konkret erhoben werden.

Online-Durchsuchung, QuellenTKÜ und QuellenTKÜ+

Durch die oben skizzierten Infektionswege und den zwingend damit einhergehenden tiefen Veränderungen in den Sicherheitsmechanismen der angegriffenen Systeme wird deutlich, dass eine technische Abgrenzung zwischen dem Staatstrojaner zur Festplatten-Durchsuchung („Online-Durchsuchung“) und dem Trojaner zum Abhören der laufenden Kommunikation („Quellen-TKÜ“) sowie der mittlerweile dritten Trojaner-Variante („Quellen-TKÜ+“ oder „Kleine Online-Durchsuchung“), die auch gespeicherte Inhalte und Umstände der Kommunikation erfassen darf, in der Praxis bei ehrlicher Betrachtung weder zuverlässig zu gewährleisten noch überhaupt klar zu umreißen ist. Die „technischen Vorkehrungen“, die alle drei Staatstrojaner-Varianten unterscheiden sollen, könnte man zwar zu implementieren versuchen, allerdings scheitert offenbar das BKA seit mehr als einem Jahrzehnt daran, Trojaner-Varianten zu entwickeln oder zu kaufen, die alle grundrechtlich gebotenen Vorgaben sicher erfüllen.

Der in § 100a Abs. 1 S. 3 StPO gezogene Vergleich zur Überwachung in öffentlichen Telekommunikationsnetzen, welcher der „Kleinen Online-Durchsuchung“ Grenzen setzen soll, kann auch deswegen nicht herangezogen werden, da auf informationstechnischen Geräten gespeicherte Daten ja gerade nicht kommuniziert werden und also keine Übertragung über Netze stattfindet. Werden lokal gespeicherte Kommunikationsinhalte ausgelesen, handelt es sich schlicht um eine „Online-Durchsuchung“.

Ein Beispiel illustriert die grundsätzlichen Probleme der Einhaltung der rechtlichen Vorgaben: Für die Überwachung beliebiger verschlüsselter Videotelefonie müssen mindestens das Mikrofon und die Kamera angezapft werden, solange die Kommunikation läuft. Die Erkennung einer laufenden Kommunikation aber muss anhand des System- und Softwareverhaltens detektiert werden und ist nicht trivial. Schlägt sie fehl und es wird aufgezeichnet, obwohl keine Kommunikation stattfindet – weil etwa das

Mikrofon softwareseitig stumm geschaltet ist oder ausschließlich Screensharing aktiviert ist, wird aus einer „Quellen-TKÜ“ eine volle Wohnraumüberwachung mit Bild und Ton.

Letztlich bleibt die Unterscheidung aller drei Trojaner-Varianten eine juristische und zudem theoretische, die mit den Realitäten der Trojaner-Branche und mit den technischen Notwendigkeiten beim erfolgreichen Infizieren eines informationstechnischen Geräts nicht zusammengehen. Da im Bereich des Einkaufs von Spionagesoftware von kommerziellen Anbietern ohnehin keine detaillierten technischen Einblicke vorgesehen sind, ist zudem eine unabhängige Prüfung der Einhaltung der „technischen Vorkehrungen“ gar nicht möglich. Das zeigt der Blick auf das bisherige Vorgehen: Lediglich „externe Prüfinstitute“ seien beispielsweise vom BKA beauftragt worden.⁵ Ob und welche Ergebnisse aus dieser Beauftragung hervorgingen, ist öffentlich nicht bekannt. Schon um angesichts solcher auch weiterhin bestehenden Unzulänglichkeiten die Einsatzzahlen von Staatstrojanern zu begrenzen, sollten höhere rechtliche Hürden zur Prüfung der technischen Details der verwendeten Trojaner festgeschrieben werden.

Die Anbieter des vom Chaos Computer Club analysierten „DigiTask“-Staatstrojaners⁶ wollten Einblicke in ihren Quellcode unter der Bedingung geben, dass eine Prüfinstanz wie der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit einen branchenüblichen Geheimhaltungsvertrag eingeht und zudem eine Gebühr bezahlt. Eine solche Quellcode-Prüfung bleibt weiterhin jedoch nicht gesetzlich vorgesehen, wäre jedoch notwendig, um die Einhaltung der rechtlichen Vorgaben prüfen zu können. Der Zugang zu Quellcode und den daraus erzeugten ausführbaren Programmen sollte künftig verpflichtend festgeschrieben werden. Eine gerichtliche Einzelfallkontrolle vor dem Einsatz oder im Nachgang einer erfolgten Überwachungsmaßnahme durch einen Staatstrojaner kann durch die typischerweise technisch nicht ausreichend vorbereiteten Richter nicht sinnvoll erfolgen. Hier bleibt man weiterhin auf die Aussagen der Anbieter angewiesen, deren Wahrheitsgehalt nicht ausreichend prüfbar sind.

Dass auf solche Aussagen von Anbietern kein Verlass ist und sie sich wegen Kompetenzmangels oder Fehlern als unwahr erweisen, zeigt der konkrete Fall der Analyse eines Staatstrojaners durch den CCC, die im Jahr 2013 dazu führte, dass das BKA keine „Quellen-TKÜ“ mehr durchführte, weil nach dieser (externen) technischen Analyse keine technisch und rechtlich korrekte Grundlage mehr gegeben war. Der damalige BMI-Staatssekretär Klaus-Dieter Fritsche musste dem Bundestag 2013 in der Folge mitteilen, dass nach „der Analyse einer Überwachungssoftware durch den CCC [...] Bund und Länder einig [seien], bis auf Weiteres auf die Durchführung von Quellen-TKÜ-

⁵ BT-Drs. 19/1434, S. 5.,

<https://dserver.bundestag.de/btd/19/014/1901434.pdf> vom 28. März 2018.

⁶ Vgl. Chaos Computer Club: Analyse einer Regierungs-Malware,

<https://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf> sowie

<https://nakedsecurity.sophos.com/2011/10/10/german-government-r2d2-trojan-faq/> vom 10. Oktober 2011.

Maßnahmen zu verzichten“.⁷ Das bedeutet zugleich, dass die durch den CCC veröffentlichten technischen Informationen zuvor in den Behörden unbekannt gewesen waren. Damals war geplant, die Entwicklungshoheit künftig bei den Behörden anzusiedeln – von dem Plan wurde offenbar später abgerückt.

Unsicherheit der Systeme nach der Infektion

Der oben umrissene komplexe Infektionsweg schwächt die Sicherheit des gesamten Systems und erleichtert damit auch anderen Angreifern den ungewollten und unbemerkten Zugang. Wie andere Angreifer auch muss die eingeschleuste Überwachungssoftware die vielfältigen, inzwischen normalen Vorkehrungen des Betriebssystems und zusätzlich installierter Abwehrwerkzeuge gegen unbefugten Zugriff auf Sensoren und Daten außerhalb des Kompartments – und deren Exfiltration – unterlaufen und ein Entdecken und Abschalten durch eine installierte Antivirus-Software verhindern.

Die verräterischen „digitalen Fingerabdrücke“ der Binärdaten des „DigiTask“-Trojaners fanden beispielsweise nach der Veröffentlichung des CCC im Handumdrehen Eingang in die meisten Datenbanken von Antivirus-Herstellern,⁸ weshalb der Einsatz dieser speziellen Spionage-Software danach wenig erfolgversprechend war. Heute versucht moderne Anti-Malware- und Antivirus-Software, die Trojaner nicht mehr nur durch direkten Vergleich mit einer Liste bekannter Software zu erkennen, sondern auch bisher unbekannte Trojaner an ungewöhnlichem Verhalten.

Daher müssen sich neuere Trojaner vor einer Entdeckung oder gar einer Deaktivierung durch geschlossene Sicherheitslücken nach regulären Software-Updates hüten. Das setzt für deren zuverlässigen und dauerhaften Betrieb eine tiefgreifende Manipulation des befallenen Systems voraus. Denn aus Sicht von Computer-Anwendern und den Herstellern von Antivirus- und Anti-Malware-Software ist der Unterschied zwischen einer staatlich eingebrachten Schadsoftware und einem kriminellen Erpressungstrojaner nur theoretisch. All dies ist im Allgemeinen nur durch ein permanentes Absenken des Sicherheitsniveaus des Gesamtsystems möglich.⁹

⁷ BT-Drs. 17/13046, S. 6.,

<https://dserver.bundestag.de/btd/17/130/1713046.pdf> vom 5. April 2013.

⁸ Vgl. Kapitel „Case R2D2“ in Mikko Hyppönen (2022): „If It's Smart, It's Vulnerable“, S. 58 f., <https://netzpolitik.org/2022/mikko-hypponen-the-first-time-we-encountered-law-enforcement-malware/> vom 3. September 2022 und <https://archive.f-secure.com/weblog/archives/00002249.html> vom 8. Oktober 2011 sowie <https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj~BckR2D2-A> vom 4. November 2011 und <https://www.virustotal.com/gui/file/be36ce1e79ba6f97038a6f9198057abecf84b38f0ebb7aaa897fd5cf385d702f/detection/f-be36ce1e79ba6f97038a6f9198057abecf84b38f0ebb7aaa897fd5cf385d702f-1318310950>

⁹ Unter Apples iOS-Betriebssystem ist der Vorgang des freiwilligen dauerhaften Ausschaltens grundlegender Sicherheitsbarrieren als „Jailbreaking“, unter Googles Android-Betriebssystem unter dem Namen „Rooting“ bekannt. Im Falle einer Infektion mit einem Trojaner findet dies unfreiwillig statt.

Doch schon das Einbringen neuer Software-Komponenten in ein System bringt erfahrungsgemäß andere, neue Problemklassen mit sich: Prinzipiell betrachtet ist keine Software ohne Fehler. Als anschauliches Beispiel können Lösungen aus dem Antivirus- und Personal-Firewall-Bereich dienen. Sie benötigen ebenfalls einen mächtigen Zugriff auf die tiefsten Funktionen des Betriebssystems. Durch ihre Komplexität werden sie regelmäßig von trickreich konstruierten Dateien aus einem Internet-Browser, einer eingehenden E-Mail oder von Daten-Paketen aus dem Internet überlistet, um diesen Produkten gewährte umfangreiche Berechtigungen gegen die Nutzer auszuspielen.¹⁰

Wie der Fall des „DigiTask“-Staatstrojaners zeigte, liefert der notwendige, sehr tiefe Eingriff einer „Quellen-TKÜ“ in das Betriebssystem eine Vielzahl von prominenten neuen Angriffsflächen an Stellen mit weitreichenden Zugriffsberechtigungen. Fällt beispielsweise ein befallenes System einer durchschnittlich begabten Hobby-Computer-Forensikerin oder einem Sicherheitsforscher aus dem Ausland in die Hände, können diese zum einen den Infektionsweg nachvollziehen und selber ausnutzen, zum anderen aber auch nach Implementierungsfehlern oder neu geschaffenen Lücken in den Trojanern selber suchen und diese auch bei einem Einsatz auf den Rechnern anderer Verdächtiger für eigene Zwecke ausnutzen und dort potentiell Daten verändern. Daher muss ein so infiziertes Gerät nach der Infiltration durch die „Quellen-TKÜ“-Komponente als potentiell von mehr als nur einem Angreifer ferngesteuert und als nicht mehr beweismäßig betrachtet werden.

Der „DigiTask“-Trojaner ist dafür ein konkretes Beispiel: Der CCC fand in seiner Analyse Fehler in der Implementierung des Protokolls für die „Command and Control“-Technik, also in dem Mechanismus, mit dem die Funktionen des Trojaners von den Behörden im Rahmen einer normalen Operation ferngesteuert werden. Durch die aufgedeckten Fehler war es beliebigen Dritten möglich, sämtliche – auch für den spezifischen Einsatz nicht erlaubte – Überwachungsfunktionen von Ferne einzuschalten und die so gewonnenen Daten auszuleiten. Dritte hätten also die „Quellen-TKÜ“ zu einer „Online-Durchsuchung“ machen können. Schlimmer noch: Ein weiterer prozessualer Fehler bei der Software-Entwicklung führte dazu, dass vor dem Einsatz durch die Behörde eine Funktion nicht abgeschaltet wurde, die es Dritten auf demselben „Command and Control“-Wege erlaubte, auf dem infizierten Zielrechner beliebige Softwarekomponenten nachträglich einzuschleusen und auszuführen.

Selbst wenn es den Herstellern möglich wäre, die An- oder Abwesenheit bestimmter Eigenschaften ihrer Software nachzuweisen, können diese Nachweise durch unabsichtliche Funktionserweiterungen von Dritten unter Ausnutzung von Sicherheitslücken im Trojaner selbst zunichte gemacht werden. Dass dabei die Software-Qualität höher und die Menge neuer ausnutzbarer Lücken geringer sein soll, als bei den vom Trojaner angegriffenen Betriebssystemen, ist zu bezweifeln.

¹⁰ Feng Xue: Attacking Antivirus, <https://www.blackhat.com/presentations/bh-europe-08/Feng-Xue/Whitepaper/bh-eu-08-xue-WP.pdf> von 2008.

Unzulässige Ausweitung der betroffenen Zielpersonen

Besonders brisant wird diese grundsätzlich unvermeidbare Schwächung der Gerätesicherheit, wenn es sich bei den betroffenen Geräten um die von „anderen Personen“ im Sinne der angegriffenen Norm handelt. Dies sind typischerweise Betreiberinnen und Administratorinnen der Dienste, die von (auch nur einem) Verdächtigen benutzt werden.

Im Leitsatz 1b in seiner Entscheidung zum BKA-Gesetz¹¹ hat das Bundesverfassungsgericht unmissverständlich klar gemacht, dass sich die Befugnisse zur Überwachung „nur unter eingeschränkten Bedingungen auf nichtverantwortliche Dritte aus dem Umfeld der Zielperson erstrecken“ dürfen. Das nun angegriffene Gesetz berücksichtigt diese Vorgabe nicht nur nicht, sondern erweitert die Zielgruppe der möglicherweise Betroffenen nun noch weit über das Umfeld der Zielperson hinaus.

Auf den zentralen Infrastrukturen der Telekommunikationsdiensteanbieter liegen die Daten vieler Nutzerinnen zusammengeführt vor. So erlaubt beispielsweise das Kompromittieren des Computers oder des Smartphones der jeweiligen Administratorinnen als „digitalem Generalschlüssel“ auch den Zugriff auf die Nutzerdaten vieler anderer auf den entsprechenden Systemen angemeldeter Nutzerinnen¹² – und dies eben nicht nur durch die im Sinne des Gesetzes zum Zugriff Befugten.

Anders ausgedrückt: Das besondere Schutzbedürfnis der Betreiberinnen und Administratoren von Kommunikationsinfrastruktur, die durch sorgfältiges Befolgen von IT-Grundschutz-Vorgaben und weiteren Regeln für eine zuverlässige IT-Sicherheit dem berechtigten Interesse der überwiegenden Zahl ihrer Nutzerinnen auf Integrität ihrer Daten nachzukommen versuchen, wird in einem Nebensatz im Gesetz konterkariert und somit eine reale Gefahr schwerer Kollateralschäden auf den Systemen der administrierten Dienste geschaffen.

Selbst wenn es möglich wäre, auf den zentralen Rechnern eines so ins Ziel genommenen Dienstes den Zugriff der bedarfstragenden Behörden für ein zielgenaues Ausspähen nur eines einzelnen Verdächtigen zu beschränken, gäbe es keinen Weg zu verhindern, dass unbefugte Dritte durch Missbrauch der neu geschaffenen Sicherheitslücken einen grenzenlosen Einblick in Inhalts- und Verkehrsdaten gewinnen. Diese technische Realität würde bei anderen Maßnahmen als geradezu absurd angesehen, etwa wenn Abhöreinrichtungen für die traditionelle Telefonüberwachung beim oder nach einem Einsatz nicht vor dem Zugriff Dritter geschützt wäre.

¹¹ 1 BvR 966/09, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/04/rs20160420_1bvr096609.html vom 20. April 2016.

¹² So etwa beim Belgacom-Hack in der „Operation Socialist“, vgl. Daniel Boffey: British spies 'hacked into Belgian telecoms firm on ministers' orders', <https://www.theguardian.com/uk-news/2018/sep/21/british-spies-hacked-into-belgacom-on-ministers-orders-claims-report> vom 21. September 2018.

Mangelnde wissenschaftliche Evaluierung

Es mangelt auch nach jahrelangem Einsatz der Staatstrojaner an einer soliden Datenlage und einer Evaluierung der technischen Umsetzung der Trojaner-Varianten sowie an einer nicht nur anekdotischen Analyse, wie sinnvoll und geeignet das staatliche Hacking ist. Der gesamte Bereich ist auch für jahrelang zurückliegende Fälle und längst überholte Spionage-Techniken nicht wissenschaftlich untersucht und von hoher Intransparenz und systematischer Geheimhaltung gekennzeichnet.

Es sollte nicht weiter hingenommen werden, dass die Aufgabe einer stichpunktartigen Prüfung an der Zivilgesellschaft hängenbleibt: Nach der öffentlichen Demontage des „DigiTask“-Trojaners durch den CCC wurde ein Produkt namens „FinSpy“ für den Einsatz beim BKA als „Quellen-TKÜ“ gekauft und geprüft. Der damalige BMI-Staatssekretär Klaus-Dieter Fritsche gab 2013 an, dass es Tests und „Quellcodeprüfungen“ gegeben habe. Ziel sei es gewesen, die Vorgaben einer „Standardisierenden Leistungsbeschreibung“ und „alle rechtlichen Vorgaben“ zu erfüllen.¹³ Das Ergebnis ist nicht öffentlich bekannt, auch nicht, ob es eine solche Quellcodeprüfung tatsächlich gegeben hat. Der CCC prüfte ein von der türkischen Regierung gegen oppositionelle Politiker eingesetztes Exemplar von „FinSpy“, das während des Einsatzes aufgefallen war, und veröffentlichte eine Analyse des Staatstrojaners.¹⁴

Im Rahmen dieser Untersuchung konnte sowohl der zur Ausweitung der Rechte notwendige Kernel-Level-Exploit „dirtycow“ nachgewiesen werden als auch der Einsatz einer gängigen Softwarekomponente namens „SuperSU“¹⁵ zum dauerhaften Herabsetzen des Sicherheitsniveaus der gehackten Geräte („Rooting“).

Ob und wie die IT-Systeme von Observationszielen nach der Maßnahme wieder in einen sicheren Zustand versetzt werden und ob dies überhaupt möglich wäre, ist genauso wenig rechtlich geregelt, wie die Mechanismen zum Schutz der ausgeleiteten Daten vor dem unbefugten Zugriff Dritter. So wurden beim 2011 vom CCC untersuchten „DigiTask“-Trojaner die ausgespähten Daten ungesichert über einen im Ausland betriebenen Server versendet. Auch der „FinSpy“-Trojaner nahm in den analysierten Varianten Verbindungen mit Servern auf, die vom Dienstleister nachträglich konfiguriert werden konnten.

¹³ BT-Drs. 17/13046, S. 5.,
<https://dserver.bundestag.de/btd/17/130/1713046.pdf> vom 5. April 2013.

¹⁴ Chaos Computer Club: Evolution einer privatwirtschaftlichen Schadsoftware für staatliche Akteure – FinFisher FinSpy für Android 2012-2019, https://www.ccc.de/system/uploads/291/original/FinSpy_Report_CCC_v1.0.pdf vom 28. Dezember 2019.

¹⁵ Vgl. <https://supersuroot.org>

Fehlendes Risikomanagement für Hacking-Werkzeuge

Für die „Quellen-TKÜ“ und für die „Quellen-TKÜ+“ sind keine gesetzlichen Schutzvorkehrungen vorgesehen, die einer Verwendung unbekannter IT-Sicherheitslücken (0-Days) zur Infiltration des informationstechnischen Systems entgegenwirken würden. Auch nachdem Staatstrojaner nun jahrelang zum Einsatz kommen dürfen, fehlt es bis heute an Vorgaben des Risikomanagements für die Hacking-Werkzeuge und damit einem definierten Prozess, der festlegt, wie mit welcher Art von Schwachstellen umzugehen ist, von denen Behörden Kenntnis erlangen. Leitlinien des Gesetzgebers, die umreißen, wie Behörden mit ihnen bekannten IT-Sicherheitslücken umgehen müssen, sollten jedoch zwingend vorgelegt werden, bevor Staatstrojaner in Umlauf gebracht werden.

Letztlich mangelt es an einer kohärenten Position der Bundesregierung zum Umgang mit IT-Sicherheitslücken durch staatliche Behörden. Die direkte und indirekte Finanzierung von professionellen Schwachstellen-Suchern, die gefundene Lücken nicht schließen lassen, sondern damit handeln und sie verkaufen, gefährdet die gesamte digitale Gesellschaft und ist auch eine Gefahr für die innere Sicherheit.

IT-Sicherheitslückenmarkt

Für den verdeckten Zugriff auf informationstechnische Systeme sind Sicherheitslücken und darauf basierende Exploits notwendig. Daraus entsteht ein Zielkonflikt: Einerseits brauchen Behörden funktionierende Exploits für Maßnahmen wie Staatstrojaner, andererseits hängt die IT-Sicherheit aller davon ab, Sicherheitslücken schnell zu schließen.

IT-Sicherheitslücken und Exploits zu kaufen und zu handeln ist im letzten Jahrzehnt zu einem lukrativen Geschäftsmodell avanciert. Insbesondere durch die Teilnahme finanzkräftiger staatlicher Behörden hat sich der entsprechende Markt im letzten Jahrzehnt signifikant vergrößert und wurde zudem indirekt legitimiert.

Dieser Markt zum Handel von IT-Sicherheitslücken und Exploits dient einerseits dem direkten Vertragsabschluss oder aber andererseits dem Zukauf von Wissen, um Spionagewerkzeuge erforschen und (weiter-)entwickeln zu können. Dies führt zu gravierenden negativen wirtschaftlichen Folgen für Deutschland und alle hochvernetzten Staaten, da das Niveau der IT-Sicherheit gesenkt wird, was auf eine nicht mehr hinnehmbare Schwächung der Informationssicherheit insgesamt hinausläuft. Da sich die Branche der Auftragshacker und auch der Ransomware-Bereich vergrößert und professionalisiert haben und zugleich abgesicherte IT-Systeme in jeder einzelnen Wirtschaftsbranche, in der Verwaltung und für Privatanwender essentiell geworden sind, sollte diese Fehlentwicklung korrigiert werden.

Neben einem schon mehrere Jahrzehnte existierenden Schwarzmarkt werden IT-Schwachstellen und Exploits mittlerweile ganz offen gehandelt. Seit 2015 wird der Staatstrojaner-Anbieter-Markt systematisch erfasst, allerdings auf diejenigen Anbieter beschränkt, deren Produkte durch Forscher analysiert

werden konnten. Das waren von 2015 bis 2021 – vor der Veröffentlichung des Pegasus-Projekts¹⁶ – knapp einhundert bekanntgewordene Staatstrojaner-Varianten weltweit.¹⁷ Im Rahmen des 2021 an die Öffentlichkeit gegangenen Pegasus-Projekts wurde die heutige deutlich vergrößerte Dimension der Branche näher beleuchtet. Die Analyse zeigt: Auch viele demokratische Staaten fördern diesen Markt aktiv und in erheblichem Umfang, um für die Nutzung von Staatstrojanern Hintertüren zu öffnen, beispielsweise für Polizeibehörden, die Informationen über Sicherheitslücken nicht selbst finden, sondern von Dritten kaufen. Mit hoher Wahrscheinlichkeit gäbe es die Schwachstellenmärkte in ihrer heutigen Form ohne die Finanzierung durch demokratische Staaten nicht.

Das oben erwähnte vom CCC untersuchte Produkt „FinSpy“ ist eine Spionagesoftware, die ursprünglich von einem Firmenkonglomerat der britischen Firma Gamma Group angeboten und etwa zehn Jahre von der deutschen FinFisher GmbH erstellt und vertrieben wurde. Wie andere Anbieter von Staatstrojanern auch stand die Gamma Group und später FinFisher in der Kritik, weil die Spionagesoftware auch an Staaten verkauft wurde, die damit Menschenrechte verletzen. „FinSpy“ wurde beispielsweise an bahrainische Behörden verkauft, die damit Dissidentinnen verfolgten und den Arabischen Frühling niederschlugen.¹⁸ Weitere Kunden der Firma waren Behörden in Diktaturen wie Dubai oder Katar, aber auch in der Mongolei und in Indonesien.¹⁹

Anbieter der Staatstrojaner bestreiten regelmäßig, ihre Produkte auch an Diktaturen zu verkaufen. Das erweist sich als kaum glaubwürdig, wie etwa die Analyse des Pegasus-Projekts und die Zeugen- und Sachverständigen-Anhörungen im Pegasus-Untersuchungsausschuss des europäischen Parlaments²⁰ ergaben. Auch das Unternehmen Hacking Team, zu deren Kunden staatliche Behörden demokratischer Staaten gehörten, verkaufte zugleich an Behörden in Ägypten, Libanon, Aserbaidschan, Kasachstan,

¹⁶ Kai Biermann, Astrid Geisler, Gero von Randow, Holger Stark, Sascha Venohr: Cyberangriff auf die Demokratie, <https://www.zeit.de/politik/ausland/2021-07/spionage-software-pegasus-cyberwaffe-ueberwachung-menschenrechte-enthuellung> vom 18. Juli 2021.

¹⁷ The Global Spyware Market Index Raw Data, https://docs.google.com/spreadsheets/d/1FHIX71XHi4U5sX8_SqebekUkMrgSKmqKoQNbANFqMlc/edit#gid=0 vom 22. Juli 2021.

¹⁸ Vgl. Andre Meister: Gamma FinFisher: Überwachungstechnologie „made in Germany“ gegen Arabischen Frühling in Bahrain eingesetzt, <https://netzpolitik.org/2014/gamma-finfisher-ueberwachungstechnologie-made-in-germany-gegen-arabischen-fruehling-in-bahrain-eingesetzt> vom 8. August 2014.

¹⁹ Vgl. Andre Meister: Gamma FinFisher: Neue Analyse des Staatstrojaners deutet auf weitere Kunden hin, <https://netzpolitik.org/2012/gamma-finfisher-neue-analyse-des-staatstrojaners-deutet-auf-weitere-kunden-hin/> vom 9. August 2012.

²⁰ Vgl. European Parliament draft recommendation to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware, https://www.europarl.europa.eu/doceo/document/B-9-2023-0260_EN.html vom 22. Mai 2023.

Sudan und Äthiopien.²¹ Diese Art Geschäftsmodell sollten deutsche Behörden grundsätzlich nicht durch ihre finanziellen Mittel unterstützen.

Zudem werden mit dem Bedienen des Marktes auch indirekt Straftaten begünstigt. Denn auch die Teile des Marktes, die ganz oder teilweise illegal und auch gesetzlich pönalisiert sind, werden stabilisiert. Und letztlich profitieren von mit Steuermitteln gekaufte Exploits mittelbar auch die organisierten Diebesbanden, die auf eigene Rechnung oder im Auftrag anderer Staaten privatwirtschaftliche, staatliche und zivilgesellschaftliche Netzteilnehmer erpressen.

Prominentestes Beispiel ist wohl die „EternalBlue“ getaufte Sicherheitslücke aus dem NSA-Arsenal, die nach einem unabsichtlichen Abfluss an eine Gruppe namens „Shadow Brokers“ im Jahr 2017 zu den bisher größten und teuersten weltweiten Ransomware-Angriffen mit den Trojanern „Wannacry“ und „Not Petya“ führten.²²

Kein „Going-dark“ ohne Staatstrojaner

Das Aufkommen von stark verbreiteten Ende-zu-Ende-verschlüsselten Kommunikationskanälen erschwert die Arbeit der Strafverfolgungsbehörden nicht in dem Maße, dass die Kryptographie -Nutzung sinnvolle Kriminalitätsbekämpfung verunmöglichen würde (sog. „Going dark“). Eine Untersuchung des Berkman Center for Internet & Society der Harvard-Universität zeigt das glatte Gegenteil:²³ Die allgemeinen informationstechnischen Entwicklungen lassen derart viele neue Informationsquellen entstehen, die von Behörden genutzt werden können, dass ein heimliches Hacken digitaler Geräte nicht notwendig ist. Die zahlreichen neuen digitalen Spuren sowie der physische Zugriff auf diese Geräte können für erfolgreiche, aber weit weniger eingriffsintensive Ermittlungen genutzt werden. Empirisch zeigt sich zudem, dass die Aktivierung der Ende-zu-Ende-Verschlüsselung durch WhatsApp für Milliarden von Accounts seit den Jahren 2015 und 2016 zu keiner Änderung in der Effizienz der Strafverfolgung führte. Neuere Studien kommen zum gleichen Ergebnis: Die hinderliche Bedeutung von verschlüsselten Kanälen und Geräten wird im Allgemeinen überbewertet.²⁴

²¹ Detlef Borchers: Überwachungssoftware: Aus Hacking Team wurde Hacked Team, <https://www.heise.de/security/meldung/Ueberwachungssoftware-Aus-Hacking-Team-wurde-Hacked-Team-2736160.html> vom 6. Juli 2015.

²² Vgl. Washington Post: NSA officials worried about the day its potent hacking tool would get loose. Then it did, https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-dbb23c75d82_story.html vom 16. Mai 2017.

²³ Bruce Schneier et al: Don't Panic: Making Progress on the „Going Dark“ Debate, Berkman Center for Internet & Society, Harvard University, <https://cyber.harvard.edu/pubrelease/dont-panic/> vom 1. Februar 2016.

²⁴ Vgl. Franziska Rau: Hindernisse für die Polizei gab es schon immer, <https://netzpolitik.org/2023/studie-ueber-going-dark-hindernisse-fuer-die-polizei-gab-es-schon-immer/> vom 19. April 2023.

Fazit

„Gegeben die technische Entwicklung, wird Freiheit und Unbeobachtbarkeit des Denkens [...] künftig untrennbar mit dem Schutz persönlichster Rechner, ihrer Anwendung und auch der Daten auf ihnen verknüpft sein. [...] Der Zugriff auf gespeicherte Computerdaten auf persönlichsten Rechnern entgegen des Willens des Eigennutzers ist daher künftig weniger mit einer klassischen Hausdurchsuchung vergleichbar, als vielmehr mit der Verabreichung bewusstseinsverändernder Drogen zum Zwecke des Erlangens von Aussagen.“²⁵ Ohne Zweifel ist das Smartphone heute für einen Großteil der Menschen ein solcher „persönlichster Rechner“, der nicht nur eine Fülle privater und höchstpersönlicher Daten zusammenzieht, sondern auch der Universalschlüssel für das digitale Leben geworden ist.

Dass mit der Änderung der Strafprozessordnung nun ein langer Katalog von Straftaten den Einsatz von Staatstrojanern gegen „persönlichste Rechner“ und viele weitere informationstechnische Systeme zulässt, ist eine eklatante Fehlentwicklung, die korrigiert werden muss. Die Integrität und Vertraulichkeit der Computersysteme von Verdächtigen und sogar faktisch unbeteiligten Betreiberinnen öffentlicher Kommunikationsinfrastruktur durch staatliche Schadsoftware absichtlich zu unterminieren, sollte vermieden werden, zumindest aber die absolute Ausnahme bleiben. Auch die mit der Änderung der Strafprozessordnung einhergehende starke Ausweitung der potentiell Betroffenen der Spionagesoftware muss reduziert werden. Auch welche konkreten Ermittlungsschwächen damit geschlossen werden sollten, bleibt nebulös, da ein „Going dark“ gar nicht belegt ist.

Die technisch unsinnige künstliche Trennung zwischen den „Payloads“ der heimlichen Infektion, die mittlerweile drei Trojaner-Varianten („Quellen-TKÜ“, „Quellen-TKÜ+“ und „Online-Durchsuchung“) mit unterschiedlichen rechtlichen Schranken hervorgebracht hat, ist Teil dieser Fehlentwicklung und ebenfalls korrekturbedürftig. Die Phantasieannahme, dass eine saubere Trennung unterschiedlicher Arten von Staatstrojanern technisch möglich wäre, muss als solche klar benannt werden.

Der starken Ausweitung der Befugnisse zum Einsatz der Staatstrojaner steht kein adäquates Korrektiv gegenüber, das fehlerhafte oder missbräuchliche Verwendung auch nur erkennen, geschweige denn abwenden könnte. Es fehlt an wirksamen Regelungen, die das Gefahrenpotential einhegen könnten. Zudem mangelt es an einer Evaluation der vergangenen Einsätze von Staatstrojanern.

Deutliche Grenzen, die das Bundesverfassungsgericht in der Vergangenheit angemahnt hat, wurden mit der Änderung der Strafprozessordnung ignoriert. In der Folge kann der Eindruck entstehen, dass eine heimliche Einbringung von Schadsoftware in Smartphones oder andere informationstechnische Systeme eine normale Art von Ermittlungsmaßnahme sein könnte. Dieser Normalisierung von Staatstrojanern sollte entschieden entgegengetreten werden.

²⁵ Andreas Pfitzmann: Rede vor dem Bundesverfassungsgericht als Sachverständiger zum Staatstrojaner, 10. Oktober 2007, Seite 3f.