Chaos Computer Club

S T E L L U N G N A H M E

zum Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen,

Drucksache 19/5412,

an den Hessischen Landtag, Innenausschuss

4. Februar 2018

Constanze Kurz, Marco Holz, Justus Hoffmann, Lukas Laufenberg

Gerne kommen wir Ihrer Bitte um Stellungnahme zum Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen nach.

Diese Stellungnahme beschäftigt mit dem geplanten Einsatz von staatlicher Spähsoftware (Staatstrojaner) zur sog. „Quellen-Telekommunikationsüberwachung“ (Quellen-TKÜ) und zur „Online-Durchsuchung“ informationstechnischer Systeme. Sie konzentriert sich auf die technischen Realitäten bei Entwicklung und Einsatz solcher Staatstrojaner und deren rechtliche, gesellschaftliche und wirtschaftliche Implikationen. Auch andere der vorgesehenen Maßnahmen im Gesetzesentwurf sind kritisch zu sehen, werden hier jedoch nicht betrachtet.

Einleitung

Der vorliegende Gesetzesentwurf bedeutet eine Ausweitung der Befugnisse des Landesamts für Verfassungschutz. Das LfV soll danach die Befugnis und die Mittel erhalten, zur Informationsgewinnung Computersysteme zu hacken.

In §§ 6 bis 9 des vorliegenden Gesetzesentwurfes ist der verdeckte Zugriff auf informationstechnische Systeme geregelt. Spionagesoftware soll dazu dienen, Computer oder andere informationstechnische Systeme dauerhaft zu infiltrieren, um Kommunikations- oder andere Daten auszuleiten. Damit greift sie in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ein. Befindet sich das angegriffene informationstechnische System in einer Wohnung, liegt zusätzlich ein Eingriff in Art. 13 Abs. 1 GG vor.

Praktisch geschieht ein solcher Zugriff, indem eine oder mehrere bestehende Sicherheitslücken ausgenutzt werden, um die Überwachungssoftware heimlich aus der Ferne oder durch direkten Zugriff auf das Gerät zu installieren und danach fest im System zu verankern. Das betroffene Endgerät ist nach dem Aufbringen des Trojaners kompromittiert, eine sichere und vertrauenswürdige Informationsverarbeitung und -übertragung nicht mehr gewährleistet. Betroffene bemerken diese Maßnahme in der Regel nicht.

Die Entwicklung eines Trojaners, der alle nötigen rechtlichen Vorgaben erfüllt, stellte Behörden in der Vergangenheit vor große Probleme. Alle bisherigen Versuche, Staatstrojaner für deutsche Behörden zu entwickeln und einzusetzen, sind entweder gescheitert oder als rechtswidrig eingestuft worden. Aktuell wird in den Medien über den Einsatz von zugekauften Trojanern des Bundeskrimininalamtes spekuliert.[1] Der in Hessen entwickelte Staatstrojaner aus dem Jahre 2011 war nicht nur rechtswidrig eingesetzt

[1] Vgl. Innenministerium gibt Staatstrojaner FinSpy offenbar frei – aber noch kein Einsatz, https://www.heise.de/newsticker/meldung/Innenministerium-gibt-Staatstrojaner-FinSpy-offenbar-frei-aber-noch-kein-Einsatz-3959660.html vom 2. Februar 2018.

worden,[2] sondern schuf auf den infiltrierten Rechnern aufgrund von groben Design- und Implementierungsfehlern weitere Lücken, die auch Dritte ausnutzen konnten.[3]

1) Risiken beim Einsatz von Staatstrojanern

1a) Ausnutzen von Sicherheitslücken

Um einen Staatstrojaner zur „Online-Durchsuchung“ oder „Quellen-TKÜ“ aus der Ferne auf ein informationstechnisches System aufspielen zu können, ist eine Sicherheitslücke erforderlich. Eine Sicherheitslücke ist in diesem Zusammenhang in der Regel ein Programmierfehler, durch den es Angreifern möglich ist, die Kontrolle über das System zu übernehmen. Sie könnenn dann beispielsweise Daten aufspielen, verändern, herunterladen oder die Funktionsweise des Systems beliebig verändern. Sicherheitslücken finden sich in zahlreicher alltäglicher Software.

Hier wird ein genereller Konflikt offenkundig, in den sich der hessische Gesetzgeber begibt: Spionagesoftware benötigt eine Schwachstelle im angegriffenen Computersystem, die vom Besitzer des Systems nicht geschlossen wurde und daher heimlich genutzt werden kann. Jeder Einsatz eines Staatstrojaners erfordert, dass eine Schadcode-Komponente unbemerkt bei der verdächtigen Person installiert wird. Denn eine Sicherheitslücke sowie der Schadcode bilden das Einfallstor für die Spionagesoftware.

Erfahren die Hersteller oder die Entwickler der betroffenen Software von einer solchen Schwachstelle, steht in der Regel nach kurzer Zeit eine Aktualisierung bereit, welche die Lücke schließt. Durch das absichtliche Offenhalten der Lücken untergräbt der Staat jene Vertrauenswürdigkeit, die er eigentlich zu schützen hat.

Zudem schafft er erhebliche sekundäre Gefahren: Werden Lücken nicht geschlossen, entsteht ein enormer Schaden für die IT-Sicherheit bei Privatpersonen und Unternehmen. Hohe Sicherheitsstandards sind gerade für Unternehmen essentiell, um keine Angriffsfläche für nachhaltig rufschädigende Datenpannen und für Wirtschaftsspionage zu bieten.[4] Darüber hinaus könnten Kriminelle oder Terroristen eine solche Lücken nutzen, um kritische Infrastruktur anzugreifen. Das Vorhandensein einer Sicherheitslücke in einer Software stellt eine Gefahr für alle Nutzer dieser Software dar.

---

[2] Vgl. LG Landshut, 4 Qs 346/10.

[3] Vgl. Chaos Computer Club analysiert Staatstrojaner, https://www.ccc.de/de/updates/2011/staatstrojaner vom 8. Oktober 2011.

[4] Vgl. IT-Sicherheitsleitfaden des Landes Hessen, https://www.hessen.de/pressearchiv/pressemitteilung/sicherheitsluecken-schaden-betrieben-0 vom 16. September 2015.

1b) Veränderte Ausgangslage bei Schadsoftware

Seit die Diskussion in Deutschland um die Einführung einer gesetzlichen Erlaubnis zum staatlichen Hacken vor mehr als zehn Jahren begann, hat sich das Gesamtbild in der IT-Sicherheit und bezüglich der Verbreitung, des Handels und der Abwehr von Schadsoftware stark gewandelt. In der jüngeren Vergangenheit ist staatliche Schadsoftware in zunehmendem Maße in die Hände Krimineller gelangt. Diese haben die Sicherheitslücken, die von staatlicher Seite geheimgehalten worden waren, genutzt, um in großem Umfang Computer mit Erpressungstrojanern[5] zu infizieren.

Das geplante Gesetz fördert den Schwarzmarkt für noch nicht geschlossene Sicherheitslücken mit Steuergeldern und erodiert damit insgesamt die IT-Sicherheit. Kriminelle profitieren von offenen Sicherheitslücken und gestohlenen Staatstrojanern – Opfer ist die Allgemeinheit.

Die internationalen Schadenssummen durch Spionagesoftware, welche von staatlichen Akteuren oder in deren Auftrag entwickelt wurde, sind stark gestiegen und liegen im Bereich von vielen Millionen Euro jedes Jahr. Nicht gemeldete Sicherheitslücken gelangten in die Hände von Dritten und schädigten in der Folge Millionen Computersysteme. Im Jahr 2017 richtete die bislang größte Welle von Schadsoftware, die aus einem staatlichen Schadsoftware-Arsenal entwendet wurde, unter dem Namen „Wannacry“ bei Unternehmen, Behörden und Privatleuten enormen Schaden an. Vergleichbares gilt für die Angriffswelle mit der Malware „NotPetya“.[6] Die Schadenssumme allein bei „Wannacry“ wird international auf über vier Milliarden Euro taxiert. Alarmierend ist dabei die Tatsache, dass in Großbritannien insbesondere Krankenhausinfrastrukturen davon betroffen und Leben und Gesundheit von Menschen gefährdet waren.

1c) Folgeschäden für Wirtschaft und Privatpersonen

Die Regelungen im Gesetzesentwurf implizieren das absichtliche Offenhalten von Sicherheitslücken in IT-Systemen durch staatliche Stellen. Gleichzeitig wird allerdings die eigentlich zwingend notwendige Einschätzung der möglichen Folgeschäden unterlassen und ist auch für den Einzelfall nicht im Gesetzesentwurf vorgesehen.

Für den Einsatz in einem Staatstrojaner sind Sicherheitslücken in besonders weitverbreiteter Software attraktiv, etwa in gängigen Betriebssystemen (Windows, Android, iOS) oder Browsern (Chrome, Firefox): Hiermit können viele verschiedene Geräte angegriffen werden, ohne den Staatstrojaner grundlegend umprogrammieren zu müssen.

---

[5] Ein Erpressungstrojaner ist eine Schadsoftware, die auf einem Rechner gespeicherte Daten verschlüsselt und erst nach Kauf eines Passworts wieder freigibt.

[6] Vgl. Ransomware-Attacke, http://www.zdnet.de/88324525/ransomware-attacke-4000-server-und-45-000-pcs-neu-installiert/ vom 26. Januar 2018.

Für Kriminelle sind solche Lücken aus demselben Grund ebenfalls interessant. Es existiert daher ein florierender Grau- und Schwarzmarkt, auf dem Informationen über Sicherheitslücken gehandelt werden. Der Staat gerät hier folglich in einen Zielkonflikt: Auf der einen Seite will er ein möglichst hohes IT-Sicherheitsniveau für Bürger und Wirtschaft garantieren; auf der anderen Seite hat er ein Interesse an offenen Sicherheitslücken in möglichst vielen und verbreiteten Systemen, um diese bei Bedarf zum Zwecke der „Online-Durchsuchung“ oder „Quellen-TKÜ“ ausnutzen zu können.

Der Weg vom staatlichen zum kriminellen Trojaner kann kurz sein, wenn die Schadsoftware abhanden kommt oder von den Überwachten auf dem eigenen Rechner entdeckt wird.[7] Da staatliche Akteure Geld für Informationen über noch unbekannte Sicherheitslücken ausgeben, um diese Lücken für Staatstrojaner nutzen zu können, wächst das Volumen der Schwarzmärkte, auf denen diese Informationen gehandelt werden. Die Hersteller der verwundbaren Software könnten diese Lücken eigentlich zum Schutz aller Nutzer bei Kenntnis durch Updates schließen. Da die Informationen über Existenz und Art der Lücke auf dem Schattenmarkt jedoch oftmals an den Meistbietenden für bis zu sechs- oder siebenstellige Eurobeträge verkauft werden, erfahren Softwarehersteller nicht von kritischen Lücken in ihren Produkten. Alle ihre Kunden bleiben damit verwundbar.

Staatliche Schadsoftware unterminiert die IT-Sicherheit damit strukturell, da ihre Entwicklung die Anreize dafür setzt, Sicherheitslücken anzubieten, zu verkaufen und nicht schließen zu lassen. Daher ist bei der Bewertung des Gesetzentwurfes nicht nur der Kostenaufwand für das Bereitstellen und den Einsatz der Software selbst zu betrachten, sondern es sind auch die Risiken zu kalkulieren, die dabei entstehen. Durch die Finanzierung und das damit einhergehende Setzen falscher Anreize beim Umgang mit Sicherheitslücken hat sich bereits eine ganze Branche entwickelt, die aktiv unser aller Sicherheit gefährdet und die Wirtschaft sowie öffentliche Stellen buchstäblich viele Millionen kostet. Eine verantwortungsvolle IT-Sicherheitspolitik zielt auf die Schließung von Lücken ab, statt sich noch an der fragwürdigen Praxis des Handels mit Schwachstellen zu beteiligen und indirekt kriminelle Händler zu unterstützen.

Der Gesetzesentwurf gibt keine Anhaltspunkte dafür, dass die dargestellten Risiken der Schadsoftware minimiert werden. Der Staat sollte seine Bürger und die Wirtschaft vor Schadsoftware schützen sowie das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme verwirklichen.[8] Das heißt ganz praktisch auch, von der Entwicklung und Finanzierung von Schadsoftware abzusehen.

---

[7] Vgl. Motherboard: Cryptocurrency Mining Malware That Uses an NSA Exploit Is On the Rise https://motherboard.vice.com/en_us/article/yw5yp7/monero-mining-wannamine-wannacry-nsa vom 30. Januar 2018.

[8] Zur allgemeinen Verbesserung der IT-Sicherheit sollten kritische Softwarekomponenten mit Hilfe öffentlicher Gelder auf Schwachstellen überprüft werden, als Vorbild könnte hier das Projekt „EU-FOSSA“ https://joinup.ec.europa.eu/collection/eu-fossa der Europäischen Kommission dienen.

An einem Großteil der heute verbreiteten Schadsoftware, die entdeckt und analysiert wurde, waren staatliche Stellen beteiligt, ob als Auftraggeber oder direkt bei der Entwicklung. Die bisher gefährlichsten bekannten Digitalwaffen („Stuxnet", „Flame", „Duqu" und „Regin") sind allesamt in staatlichem Auftrag entstanden.[9] Mittelbar trägt der Staat als Auftraggeber damit eine Mitschuld an der Existenz und Verbreitung solcher Digitalwaffen.

Die Auswirkungen von staatlich finanzierter Entwicklung von Schadsoftware, die sämtliche Bereiche der Wirtschaft, die öffentliche Infrastruktur und Millionen Privatleute gefährdet, können nicht mehr ignoriert werden, wenn sich nun das Bundesland Hessen anschickt, ebenfalls eine gesetzliche Grundlage zu schaffen, die diese Fehlentwicklung vorantreiben wird. Denn die Entwicklung von Spionagesoftware kann leicht zum Boomerang werden, wenn die Malware den Besitzer wechselt.

Der Zweitverwertungsmarkt für Sicherheitslücken und Trojaner ist erheblich angewachsen. So könnten auch repressive Regimes im Ausland die von Steuergeldern in Deutschland finanzierten Hacking-Tools zum Ausspähen von Journalisten, Oppositionspolitikern und unterdrückten Minderheiten nutzen.[10] Die Technologie-Zulieferer solcher Regierungen sitzen oft in Europa, wirksame Exportverbote gibt es bisher nicht.[11]

Prinzipiell ist das Ausnutzen von Sicherheitslücken von staatlicher Seite nicht wünschenswert, da es im Interesse aller Behörden liegen sollte, diese Lücken konsequent und zeitnah schließen zu lassen. Das Interesse von Behörden muss es nicht nur sein, die eigenen Systeme zu sichern, sondern auch Folgeschäden ihres Tuns für Wirtschaft und Privatpersonen zu vermeiden. Einem Fortbestand von Sicherheitslücken, die staatlichen Stellen bekanntgeworden sind, muss daher konsequent entgegengewirkt werden. Dazu muss in den Gesetzesentwurf mindestens eine Meldepflicht für das LfV aufgenommen werden, insbesondere bei Sicherheitslücken, die in weitverbreiteter und sicherheitskritischer Software bestehen. Solche Lücken stellen eine enorme Gefährdung für eine große Zahl von Geräten dar.

Warum in Hessen oder in Deutschland finanzierte Hacking-Tools gegen eine spätere missbräuchliche Nutzung besser geschützt sein sollen als etwa die Arsenale von anderen Geheimdiensten, ist nicht ersichtlich.[12]

---

[9] Vgl. Regin: Top-tier espionage tool enables stealthy surveillance, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/regin-analysis.pdf vom 27. August 2015.

[10] Vgl. etwa bei der Spähsoftware Pegasus, https://citizenlab.ca/2017/07/mexico-disappearances-nso/ vom 10. Juli 2017.

[11] Vgl. Europas Exportkontrollen für digitale Waffen versagen, http://www.zeit.de/digital/datenschutz/2017-02/ueberwachung-technik-exporte-europa-kontrolle-versagt vom 24. Februar 2017.

[12] Auch finanziell und personell gut ausgestatteten Behörden wie der NSA ist es wiederholt nicht gelungen, die Geheimhaltung der von ihnen genutzten Spionagesoftware sicherzustellen, vgl. Hackers Stole NSA Cybertools In Another Breach Via Another Contractor, https://www.npr.org/2017/10/05/555922305/report-hackers-stole-nsa-cybertools-in-another-breach-via-another-contractor vom 5. Oktober 2017 sowie NSA's EternalBlue exploit, http://www.zdnet.com/article/a-giant-botnet-is-forcing-windows-servers-to-mine-cryptocurrency/ vom 1. Februar 2018.

Im Gesetzesentwurf fehlt eine Regelung, die fordert, eine genutzte Schwachstelle und die zugehörige Schadsoftware im Einzelfall einem Richter oder einer anderen unabhängigen Stelle vorzulegen sowie eine Prognose zu erstellen, ob die jeweilige Schwachstelle dazu geeignet ist, bei Geheimhaltung einen großen Anteil der Bevölkerung, kritische Infrastrukturen oder die Wirtschaft in besonderer Weise zu schädigen. Ohne eine solche Prüfung, und zwar bevor die Lücke in einem Trojaner genutzt wird, kann die Wahrscheinlichkeit von eintretenden Pannen und Zweckentfremdungen des Trojaners nicht reduziert werden. Zusätzlich kann eine derartige Regelung im Missbrauchsfall Verantwortlichkeiten klären.

1d) Missbrauchsprävention

Missbrauchsfälle sind nicht theoretisch. Die umfassende Spionage, die durch einen Staatstrojaner ermöglicht wird, ist geeignet, Menschen mit Informationen zu erpressen oder ihnen durch Identitätsdiebstahl Schaden zuzufügen. Im Rahmen der Snowden-Veröffentlichungen war bekanntgeworden, dass NSA-Mitarbeiter ihre Spionagewerkzeuge routinemäßig für private Zwecke missbraucht haben.[13] Öffentlich bekannte Fälle in Deutschland betrafen etwa Polizeibehörden, die Staatstrojaner einsetzten.[14]

Für Geheimdienste wie das Landesamt für Verfassungsschutz, die weniger öffentlichen und justiziellen Kontrollen unterliegen als Polizeibehörden, muss ein höheres Schutzniveau gegen Missbrauch angestrebt werden. Aus den Fällen in der Vergangenheit sollte die Lehre gezogen werden, dass eine Spionagesoftware wie ein Staatstrojaner in keinem Fall durch Einzelpersonen im LfV missbräuchlich nutzbar sein darf. Entsprechende Maßnahmen und konkrete Lösungsansätze, die dem entgegenwirken, fehlen im Gesetzesentwurf.

Gefährdet ist auch der Hessische Landtag selbst sowie die Mitglieder des Parlamentarischen Kontrollgremiums, die zur Erfüllung ihrer Aufgaben ebenfalls verbreitete Standardsoftware einsetzen. Das ist genau die Art von Software, die primäres Ziel eines Staatstrojaners ist. Der vom Parlament kontrollierte Geheimdienst wird mit dem Gesetzesentwurf quasi in die Lage versetzt, die eigene Kontrollinstanz zu hacken. Auch dieses Risiko ist nicht

---

[13] Vgl. NSA staff used spy tools on spouses, ex-lovers, https://www.reuters.com/article/us-usa-surveillance-watchdog/nsa-staff-used-spy-tools-on-spouses-ex-lovers-watchdog-idUSBRE98Q14G20130927 vom 27. September 2013.

[14] In der „Patras"-Affäre war 2012 bekanntgeworden, dass ein Polizeibeamter eine Schadsoftware der Bundespolizei zur Überwachung seiner jugendlichen Tochter zweckentfremdet hatte. Auf deren Rechner war der Trojaner später von einem Freund entdeckt worden, dem es in der Folge gelang, Systeme der Bundespolizei zu kompromittieren. Vgl. Patras – Vater-Tochter-Streit löst Angriff auf Bundespolizei aus, https://www.golem.de/1201/88870.html vom 8. Januar 2012.

theoretisch, sondern wurde von „befreundeten“ Geheimdiensten bereits praktiziert.[15]

Abschließend bleibt festzustellen, dass im Entwurf zum Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen keine Vorkehrungen geschaffen werden, die einem Missbrauch aktiv entgegenarbeiten oder anderweitig risikomindernd wirken. Das LfV soll zwar unter bestimmten Bedingungen Computer und weitere informationstechnische Systeme ausspähen dürfen, allerdings keinen speziellen Regelungen unterworfen werden, die einem Missbrauch präventiv begegnen.

2) Staatstrojaner im hessischen Gesetzesentwurf

2a) Begrenzung auf laufende Gespräche bei der „Quellen-TKÜ“

Im Zielsystem vorhandene Schwachstellen werden sowohl für die „Quellen-Telekommunikationsüberwachung“ nach § 6 Abs. 2, dessen Funktionsumfang auf das Abhören von Gesprächen reduziert sein soll, als auch für die „Online-Durchsuchung“ des gesamten informationstechnischen Systems nach § 8 benötigt. Beide Maßnahmen unterscheiden sich nur im Umfang der abgegriffenen Daten. Die Notwendigkeit der Kompromittierung der Systeme ist bei „Online-Durchsuchung“ und „Quellen-TKÜ“ technisch identisch.

Aus technischer Sicht bestehen erhebliche Zweifel daran, ob die Überwachung bei der sogenannten „Quellen-TKÜ“ präzise auf laufende Gespräche eingrenzbar ist. Die Frage, wie laufende Kommunikation treffsicher von anderen auf dem Gerät stattfindenden Datenverarbeitungsprozessen unterschieden werden kann, ist technisch nicht befriedigend gelöst. Der Grund dafür ist, dass eine Bestimmung, wann eine Äußerung an einem Computer zu einer Kommunikation wird, nicht immer leicht zu treffen ist: Praxisnahe Beispiele dafür sind der Entwurf einer E-Mail, die vom informationstechnischen System erfasst, aber nie gesendet wird, oder das Eintippen einer Whatsapp-Nachricht, ohne diese abzusenden. Wird im Rahmen einer „Quellen-TKÜ“ ein solcher nicht gesendeter Entwurf erfasst, handelt es sich jedoch nicht um Kommunikation, sondern gleichsam um das Festhalten von Gedanken. Praktisch geschieht dies etwa, wenn die Spionagesoftware Bildschirmfotos anfertigt, wie es von Staatstrojanern zur „Quellen-TKÜ“ in der Vergangenheit bereits durchgeführt wurde.

Der hessische Gesetzgeber versucht bei der Regelung zur „Quellen-TKÜ“ den gefährlichen Irrweg zu beschreiten, den schon der Bundesgesetzgeber in der Neuregelung des Staatstrojaners in der Strafprozessordnung beschritten hat: Er behandelt das staatliche Hacken eines informationstechnischen Geräts für den Fall der „Quellen-TKÜ“ als eine Art Fortschreibung der herkömmlichen Telekommunikationsüberwachung. Diese unterscheidet

---

[15] Vgl. CIA admits to spying on Senate staffers, https://www.theguardian.com/world/2014/jul/31/cia-admits-spying-senate-staffers vom 31. Juli 2014.

sich technisch gesehen jedoch fundamental von einer Spionagesoftware, da erstere mit Hilfe des Kommunikationsanbieters durchgeführt wird. Die „Quellen-TKÜ“ ist hingegen ein Einbruch in ein Computersystem mit allen damit einhergehenden Risiken und Nebenwirkungen und darf daher nicht als bloße Telekommunikationsüberwachung missverstanden werden. Eine rechtliche Gleichsetzung beider Maßnahmen verbietet sich daher.

2b) Vorgesehene Bedingungen zur „Online-Durchsuchung“

Der hessische Gesetzesentwurf missachtet das Urteil des Bundesverfassungsgerichts, das den Einsatz von Staatstrojanern an Bedingungen knüpft: „Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen“.[16] Im vorliegenden Gesetzesentwurf erfolgt diese Einschränkung im Bezug auf die „Online-Durchsuchung“ nicht. Insbesondere erfolgt noch nicht einmal eine Einschränkung auf Straftaten nach § 3 Abs. 1 des G10-Gesetzes, wie es für die „Quellen-TKÜ“ nach § 6 der Fall ist. Fragwürdig ist zudem, ob die Maßgabe einer „dringenden Gefahr für Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist“ nach § 7 für Wohnraumüberwachung und „Online-Durchsuchung“ mit Blick auf das Urteil rechtmäßig ist. Die Erlaubnis des Trojaner-Einsatzes bei „Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist“, stellt eine erhebliche Erweiterung dar und ist zu weitgehend.

Betrachtet man zudem die Realität des Einsatzes eines Staatstrojaners, ist es ohnehin widersinnig, einen Landesgeheimdienst mit der Aufgabe der Infektion eines Computersystems zu betrauen, wenn eine konkrete Gefahr für ein überragend wichtiges Rechtsgut droht. Denn das staatliche Hacken benötigt eine Reihe von vorbereitenden Handlungen und das Sammeln von Informationen über das anzugreifende System. Die Installation der Schadsoftware muss immer vorbereitet werden, damit das Zielsystem analysiert, sicher identifiziert und entlang der rechtlichen Vorgaben dann infiziert werden kann.

Diese Prozeduren sind zeitaufwendig und daher bei Gefahr im Verzug nicht mehr sinnvoll durchführbar, wenn es um eine konkrete Gefahrensituation geht, in der ein überragend wichtiges Rechtsgut wie beispielweise ein Menschenleben bedroht ist. Zwar kann nach § 9 Abs. 1 bei „Gefahr im Verzug“ auf den eigentlich vorab vorgesehenen Richtervorbehalt verzichtet und der Trojanereinsatz stattdessen erst einmal von der Behördenleitung genehmigt werden, der Staatstrojaner ist als Ultima Ratio zum Schutz vor konkreten Gefahren aber aufgrund der nötigen Vorlaufzeiten kein geeignetes Mittel.

---

[16] Urteil des Ersten Senats vom 27. Februar 2008, 1 BvR 370/07, 1 BvR 595/07, 2. Leitsatz.

Genauso ist ein Geheimdienst in solchen Fällen nicht die adäquate Behörde, die eingeschaltet werden sollte.

Das staatliche Hacken weiter in den präventiven Bereich auszudehnen, widerspricht den Vorgaben des Bundesverfassungsgerichts. Das LfV ist schon wegen seiner typischen Aufgaben keine geeignete Behörde, um Staatstrojaner einzusetzen. Denn wenn wie vom Bundesverfassungsgericht gefordert, die „Online-Durchsuchung“ auf die Abwehr von Gefahren für Leib und Leben zu beschränken ist, sollten solche Situationen nicht dem LfV überlassen werden.

2c) Trennungsgebot zwischen polizeilicher und geheimdienstlicher Arbeit

Der Gesetzesentwurf sieht in § 21 Abs. 2 vor, dass Abhör-Daten des LfV an andere Behörden weitergegeben werden können. Dadurch ist das Trennungsgebot tangiert, das geheimdienstliche von polizeilicher Arbeit abkoppeln soll. Folge der Regelung zu den Datenaustauschmöglichkeiten ist eine Aushebelung datenschutzrechtlicher Schutzvorschriften.

Das Trennungsgebot kann auch berührt sein, wenn im LfV die vom Bundeskriminalamt entwickelte Software „Remote Communication Interception Software“ mitbenutzt werden sollte. Es ist inakzeptabel, dass gemäß dem Gesetzesentwurf nicht dokumentiert werden muss, welche Spionagesoftware vom LfV verwendet wird, insbesondere bei der Mitwirkung externer Dienstleister. Ebenfalls fehlt ein Verbot zur Zusammenarbeit mit Unternehmen, die ihre Hacking-Werkzeuge auch an Staaten anbieten, die Menschenrechte und demokratische Standards missachten.

2d) Richtervorbehalt und Prüfung

Nach dem Gesetzesentwurf soll ein Richter gemäß § 9 den Einsatz der Schadsoftware kontrollieren. Konkret ist für diese Prüfung das Amtsgericht Wiesbaden vorgesehen. Eine besondere Qualifikation, um die technische Wirkmächtigkeit des Spionagewerkzeugs sowie die praktischen Abläufe zu verstehen, ist dabei nicht vorgesehen. Das gilt auch für die zweite richterliche Prüfung bei der Verwertung der erhobenen Daten.

Eine Rechtmäßigkeitsüberprüfung durch Richter erfordert auch eine technische Prüfung des Trojaners. Diese ist ohne eine Pflicht zum Hinterlegen des Trojaners samt Quelltext nicht möglich. Das dient zugleich der Qualitätssicherung, um rechtlichen und technischen Problemen aufgrund schlampiger und fehlerhafter Programmierung vorzubeugen, die in früher

eingesetzten Versionen von Staatstrojanern der Firma Digitask mit Sitz in Haiger (Lahn-Dill-Kreis) belegt wurden.[17]

Desweiteren fehlt auch eine Regelung, dass dem Verfassungsschutz der Quelltext des Trojaners überhaupt bekannt sein muss. Es ist zu befürchten, dass wie in der Vergangenheit proprietäte Software von kommerziellen Anbietern eingekauft wird, die aufgrund schlampiger Programmierung selbst unsicher ist und die zugehörigen Serverssysteme des Landesamts für Verfassungsschutz selbst angreifbar macht. Trotz dieser Gefahren ist eine Dokumentation auch durch eventuell hinzugezogene externe Dienstleister nicht vorgeschrieben.

Den Richtern des Amtsgerichts Wiesbaden wird die Verantwortung für Entscheidungen auferlegt, die ohne Kenntnis des technischen Sachverhaltes aber gar nicht adäquat zu treffen sind. Der Gesetzesentwurf verkennt die Notwendigkeit technischer Kenntnisse zur rechtlichen Bewertung des Trojanereinsatzes, so dass sich die Richter auf die Aussagen von Mitarbeitern des LfV oder deren externer Dienstleister verlassen müssen. Zudem ist wegen der vorab vorzunehmenden Kernbereichsprognose bei Einsatz des Spionageprogramms eine Kammer einem einzelnen Richter vorzuziehen.

Die technische Prüfung, ob mittels Staatstrojaner erhobene Daten authentisch (und damit nach Weitergabe an Polizeibehörden oder Staatsanwaltschaften gemäß § 21 Abs. 2 in einem Gerichtsverfahren verwertbar) sind, dürfte in den meisten Fällen unmöglich sein: Dass der Zugriff mittels Staatstrojaner über eine Sicherheitslücke möglich war, beweist schließlich, dass das Gerät zu diesem Zeitpunkt kompromittierbar war. Es ist daher nicht nachweisbar, ob gefundene Beweise tatsächlich vom überwachten Nutzer stammen oder von Dritten dort hinterlegt oder manipuliert wurden.

2e) Rechtsstaatliche Kontrolle und Prüfung

Der Gesetzesentwurf wirft die generelle Problematik der Prüfung der Rechtmäßigkeit bei konkreten Einsätzen des Staatstrojaners durch den hessischen Verfassungsschutz auf. Anders als in der Polizeiarbeit, bei der regelmäßig Ermittlungsmethoden der Prüfung durch Gerichte, Strafverteidiger und die Beschuldigten selbst stattfinden, arbeitet ein Geheimdienst unter weit geringerer öffentlicher Kontrolle. Vergangene Geheimdienstskandale lassen auch nicht erkennen, warum der hessischen Behörde ein besonderes Vertrauen entgegengebracht werden sollte. Das hessische LfV hat im Rahmen des parlamentarischen Untersuchungsausschusses im Wiesbadener Landtag zum NSU-Skandal und zum ehemaligem V-Mann-Führer Andreas Temme wenig Anlass für Vertrauensvorschuss geboten.

---

[17] Vgl. Chaos Computer Club analysiert Staatstrojaner, http://ccc.de/de/updates/2011/staatstrojaner vom 27. Juni 2012.

Ein Aspekt der Prüfung des rechtmäßigen Einsatzes ist die Aufzeichnung der Verfahrensschritte. Die im Gesetzesentwurf vorgesehene Protokollierung von „nichtflüchtigen Änderungen“ nach § 6 Abs. 4 Satz 1 Nr. 5 ist unzureichend. Eine Änderung ist im technischen Sinne „flüchtig“, wenn sie nur auf den Arbeitsspeicher des Rechners angewendet wird. Dieser wird normalerweise beim Herunterfahren oder Neustarten des Systems verworfen. Demgegenüber stehen nichtflüchtige Änderungen, welche auf Festplatten, SSDs oder Speicherkarten angewendet werden. Diese Speichermedien behalten ihre Daten auch dann, wenn das Gerät ausgeschaltet wird. Eine „nichtflüchtige“ Änderung bleibt also auf unbegrenzte Zeit bestehen.

Eine eindeutige Trennung zwischen flüchtigen und nichtflüchtigen Änderungen ist beim Trojanereinsatz in der Praxis jedoch aus zweierlei Gründen nicht möglich: Zum einen werden die meisten Smartphones, Server und Router sowie viele PCs und Laptops selten oder nie neu gestartet.[18] Eine technisch gesehen „flüchtige“ Änderung kann deshalb monate- oder jahrelang fortbestehen. Zum anderen sind die Systeme, in die der Verfassungsschutz mit dem Trojaner einbrechen soll, so komplex, dass es nicht möglich ist, alle Wechselwirkungen zwischen Trojaner und angegriffenem System abzusehen. Das versehentliche Hinterlassen von nichtflüchtigen Veränderungen durch den Verfassungsschutz ist daher sehr wahrscheinlich.

Folglich könnte ein von staatlichen Stellen eingesetzter Trojaner erhebliche Veränderungen am System vornehmen, die nicht von der Protokollierungspflicht nach § 6 (4) umfasst wären. Dass flüchtige Veränderungen generell nicht dokumentiert werden müssen, ist daher unzureichend. Hierbei ist auch zu bedenken, dass mittlerweile Schadsoftware im Umlauf ist, die sich ausschließlich im flüchtigen Speicher des Systems aufhält. Das zeigt, dass eine Schadsoftware nicht weniger problematisch ist, nur weil sie im technischen Sinne „flüchtig“ ist.

Der vorliegende Gesetzesentwurf liefert keine ausreichenden Regelungen zur besonderen rechtsstaatlichen Kontrolle des Einsatzes von geheimdienstlichen Trojanern. Für Maßnahmen nach § 6 Abs. 2 des Verfassungschutzgesetzes („Quellen-TKÜ“ mit Trojanereinsatz) sind im Verfassungschutzkontrollgesetz keine Berichtspflichten an das parlamentarische Kontrollgremium vorgesehen.

In § 6 Abs. 4 werden keine Dokumentationspflichten über die Herkunft der genutzten Sicherheitslücke und ggf. der Vertragspartner bzw. die unterstützende Behörde bei Zulieferung der Spionagesoftware angeführt. Das Kontrollgremium und der hessische Datenschutzbeauftragte können somit keinen Einblick nehmen und die Gefahren für Privatpersonen und Wirtschaft durch das Ausnutzen der Sicherheitslücke nicht einschätzen.

---

[18] Das Aktivieren des Ruhezustands ist kein Ausschalten des Systems. Hierbei wird der Inhalt des flüchtigen Speichers auf den nichtflüchtigen Speicher kopiert und nachträglicher Analyse sogar nach einem späteren Ausschalten zugänglich gemacht.

Wie bei jeder geheimen Überwachung sollte sich das LfV einer unabhängigen Kontrolle stellen müssen: sowohl bei Entwicklung und Nutzung von Trojanern als auch durch gerichtliche Prüfung der Einsatzprotokolle. Welche Daten von den Geräten gewonnen oder in diese eingespielt und welche konkreten Maßnahmen ergriffen wurden, um einen Missbrauch der Spionagesoftware durch Dritte zu vermeiden, muss im Einzelfall dokumentiert werden.

Diese Dokumentation wäre zudem einer Evaluation des Gesetzes dienlich, welche aufgrund der Schwere der vorgesehenen Grundrechtseingriffe dringend geboten ist. Eine Befristung des Gesetzes ist daher sinnvoll und würde spätere Korrekturen auf der Basis dokumentierter Fakten ermöglichen.

2f) Besondere Benachteiligung von Menschen mit Behinderung

Generell finden sich keine Regelungen zur Sicherstellung der Integrität und Funktionalität des betroffenen informationstechnischen Systems im Gesetzesentwurf. Wie bereits vom Arbeitskreis barrierefreies Internet e. V. kritisiert,[19] stellt dies eine besondere Beeinträchtigung Behinderter dar, da Veränderungen an Systemen mit spezialisierter Software schnell dazu führen können, dass diese Systeme aufgrund des Verlusts der Barrierefreiheit nicht mehr genutzt werden können. Da sich sowohl Überwachungssoftware als auch sog. Screenreader („Bildschirmvorleser“) und vergleichbare Assistenzsysteme in dieselben Schnittstellen des Betriebsystems integrieren, wäre hier eine Software-Inkompatabilität denkbar und nicht unwahrscheinlich. Anders als unter Punkt G auf Seite 3 des Gesetzesentwurfs behauptet, liegen demnach besondere Auswirkungen auf behinderte Menschen vor. Hier ist eine erneute Prüfung des Entwurfs nach den Maßstäben der UN-Behindertenrechtskonvention nötig.

Darüber hinaus sei darauf hingewiesen, dass eine Beeinträchtigung der Funktionalität des kompromittierten informationstechnischen Systems dazu führen wird, dass der Einsatz der Software zur „Online-Durchsuchung“ bzw. „Quellen-TKÜ“ nicht unbemerkt bleibt. Sowohl die Maßnahme an sich als auch die vom Trojaner genutzte Sicherheitslücke könnten dadurch öffentlich werden.[20]

---

[19] Vgl. Arbeitskreis barrierefreies Internet e. V.: Hessentrojaner bedroht Behinderte, http://akbi.de/2017/12/22/pm-37-hessentrojaner-bedroht-behinderte-akbi-schliesst-sich-gemeinsamer-erklaerung-gegen-verfassungsschutzgeset-z-an/ vom 22. Dezember 2017.

[20] Zur Gefahr für die Bevölkerung durch offene Sicherheitslücken in kritischer Infrastruktur siehe auch Abschnitt 1c, Seite 4.

2g) Unverhältnismäßige Grundrechtseingriffe

Aufgrund der zentralen Rolle, die insbesondere Smartphones für die höchstpersönlichen Beziehungen vieler Menschen spielen, darf die „Quellen-TKÜ“ nicht als eine Fortsetzung der Telefonüberwachung mit anderen Mitteln missverstanden werden (vgl. Abschnitt 2a, S. 8f.). Wenn eine staatliche Stelle durch Schadsoftware den Zugriff auf ein Smartphone erlangt, ist das nicht einfach nur das Äquivalent einer abgehörten Telefonleitung. Das digitale Abbild vieler Lebensaspekte der Person ist mit dem informationstechnischen System verbunden: höchstpersönliche Gespräche mit Partnern, Familienmitgliedern und Freunden, besuchte Webseiten, Suchbegriffe und Aufenthaltsorte.

Beispielhaft zu bedenken ist hier, dass Menschen auch intime Beziehungen über informationstechnische Systeme anbahnen und private Nachrichten als Texte, Bilder oder Videos mit höchstpersönlichem Inhalt mittels Computern und Smartphones erstellen und versenden. Ähnliches gilt für das Teilen und Diskutieren religiöser und weltanschaulicher Überzeugungen oder die vertrauliche Kommunikation mit Geistlichen oder Berufsgeheimnisträgern. Es ist unvermeidbar, dass derartige Nachrichten bei einer „Online-Durchsuchung“ oder „Quellen-TKÜ“ ebenfalls erfasst werden können.

Eingriffe in den besonders geschützten Kernbereich der privaten Lebensgestaltung müssen zum einen wirksam verhindert werden. Zum anderen müssen kernbreichsrelevante Daten zusätzlich gegen missbräuchliche Verwendung gesichert werden. Fälle, in denen derartige Überwachungsinstrumente missbraucht wurden, sind nicht theoretisch und bei „befreundeten“ Geheimdiensten auch öffentlich geworden.[21] Der damalige Datenschutzbeauftragte Peter Schaar hat in seinem Bericht über „Maßnahmen der Quellen-Telekommunikationsüberwachung bei den Sicherheitsbehörden des Bundes“ in deutlichen Worten bemängelt, dass bei einem mittels „Quellen-TKÜ“ abgehörten Skype-Gespäch rechtswidrig auch Liebesbeteuerungen, erotische Gespräche und Selbstbefriedigungshandlungen abgehört und sogar noch gespeichert und protokolliert worden waren.[22]

Manche Kommunikationsendgeräte werden von mehreren Personen verwendet. Damit sind beim Trojanereinsatz auch deren Grundrechte zu berücksichtigen. Es ist für einen Überwachungstrojaner nicht erkennbar, wer gerade vor dem Gerät sitzt. Wird also der Computer einer Zielperson mit einem Trojaner infiziert, können private Daten von Dritten ebenfalls betroffen sein, ebenso wird ein Eingriff in deren höchstpersönlichen Lebensbereich möglich.

---

[21] In NSA-Büros wurden intime Fotos abgefangen und herumgereicht, vgl. The NSA Shared Sexually Explicit Photographs, Says Edward Snowden, http://time.com/3010649/nsa-sexually-explicit-photographs-snowden/ vom 21. Juli 2014.

[22] Vgl. Bericht von Peter Schaar, abrufbar unter https://www.ccc.de/system/uploads/103/original/Schaar-Bericht.pdf vom 31. Januar 2012.

2h) Zugriff auf beliebige informationstechnische Systeme

Dem Gesetzesentwurf fehlt in den §§ 6 und 8 eine Eingrenzung der informationstechnischen Systeme, in die eingegriffen werden darf. Aufgrund der immer weiter zunehmenden Vernetzung von Gebrauchsgegenständen und medizinischen Geräten erscheint eine Einschränkung jedoch zwingend nötig. Ein Eingriff in Systeme mit Bezug zu kritischer Infrastruktur (etwa Stromnetze, Internetknotenpunkte), aber auch beispielsweise Industrieanlagen und Maschinensteuerungen, Fahrzeugelektronik, Behördennetze sowie medizinisch genutzte Computersysteme (Herzschrittmacher, lebenserhaltende Maschinen, elektronische Implantate) ist mit unkalkulierbaren Risiken für die Betroffenen oder gar für die gesamte Bevölkerung verbunden. Eine solche Maßnahme sollte daher vom Gesetzgeber präventiv unterbunden werden. Beim Einsatz von Schadsoftware bleibt jedoch immer ein Restrisiko, auch solche Systeme versehentlich zu beeinträchtigen.

Der Gesetzesentwurf erlaubt nach §§ 6 und 8 die Kompromittierung informationstechnischer Systeme Dritter, sofern diese Systeme durch von der Maßnahme betroffenen Personen genutzt werden. Hier liegt nicht nur ein gravierender Eingriff in die Rechte einzelner Dritter vor. Dies kann auch Systeme betreffen, die von einer größeren Anzahl von Personen genutzt werden, etwa Serversysteme wie E-Mail-Server. Die Gefährdung der Funktionsfähigkeit und auch die Erfassung von Daten vieler Unbeteiligter kann dabei nicht ausgeschlossen werden soll. Eine definitorische Beschränkung ist daher in den Gesetzesentwurf aufzunehmen.

In § 8 liegt zudem gar keine Eingrenzung der zu kompromittierenden Systeme vor, so dass nicht einmal die Nutzung des informationstechnischen Systems durch Zielpersonen Bedingung für einen Eingriff ist. Nach den Vorausetzungen des § 3 Abs. 2 des G10-Gesetzes können sich die getroffenen Maßnahmen auch „gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Verdächtigen bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben“. Diese Regelung war ursprünglich für die Telekommunikationsüberwachung ohne den Einsatz von Staatstrojanern vorgesehen. Sie ist zu weitgehend, wenn sie ebenfalls auf die aktive Kompromittierung von Computersystemen unbeteiligter Dritter (etwa auch Internetdiensteanbieter) angewandt wird. Dieses Problem wird dadurch verstärkt, dass ein bloßer Verdacht, auf einem System könnten sich relevante Daten befinden, zur Anwendung der Trojaner-Maßnahme ausreicht. Eine Schadsoftware in ein solches System einzuspielen, gefährdet jedoch die Sicherheit aller seiner Nutzer und nimmt Grundrechtsverletzungen bei völlig unbeteiligten Personen billigend in Kauf.

Zusammenfassung

Nach dem geplanten Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen soll das LfV die Befugnis erhalten, sich heimlich in Computersysteme zu hacken. Sowohl der Einsatz als auch die Entwicklung der dafür benötigten Schadprogramme bringen erhebliche Gefahren mit sich, denen der Gesetzesentwurf nur unzureichend Rechnung trägt.

Da für Trojaner Sicherheitslücken benötigt werden, müssen diese gefunden oder erworben werden. Solche Sicherheitslücken, die absichtlich geheimgehalten werden, stellen eine erhebliche Gefährdung für kritische Infrastrukturen, Behörden, Wirtschaft und Privatpersonen dar. Vorfälle wie die rasante Ausbreitung der Schadsoftware „Wannacry“, bei der eine von der NSA geheimgehaltene Sicherheitslücke ausgenutzt wurde, zeigen, wie unmittelbar diese Bedrohung ist. Im Gesetzesentwurf fehlen Maßnahmen, die diese Risiken mindern könnten. Dem Missbrauch von staatlicher Schadsoftware wird zudem nicht ausreichend vorgebeugt. Eine wirksame Kontrolle des Trojanereinsatzes kann aufgrund lückenhafter Protokollierungspflichten nicht erfolgen.

Die Eingriffshürden für Maßnahmen nach §§ 6 und 8 („Quellen-TKÜ“ und „Online-Durchsuchung“) sind nicht ausreichend. Angesichts der Schwere der Grundrechtseingriffe, auch in den Kernbereich der privaten Lebensgestaltung, wären Nachbesserungen am Gesetzesentwurf zwingend.

Die Entwicklung und der Einsatz von Schadsoftware durch den Staat sind aufgrund der dargestellten erheblichen und strukturellen Risiken für die IT-Sicherheit auch grundsätzlich abzulehnen. Die entsprechenden Paragraphen sind zu streichen.