VERBAND DER INTERNETWIRTSCHAFT E.V.

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)772 D

Kurzkommentierung zum Entwurf eines Gesetzes zur Modernisierung der Rechtsgrundlagen der Bundespolizei (BT-Drs. 19/26541)

Berlin, 19.03.2021

Im Rahmen des Gesetzesvorhabens soll der Bundespolizei u. a. die Befugnis zum Einsatz eines Staatstrojaners im Bereich der Gefahrenabwehr eingeräumt werden.

eco sieht den Einsatz von Trojanern grundsätzlichen kritisch und lehnt diesen aufgrund der damit verbundenen Auswirkungen und Implikationen ab. Trojaner gefährden die IT-Sicherheit von Bürgern, Wirtschaft und des Staates selbst. Sie höhlen die Vertrauenswürdigkeit von Kommunikation aus und gefährden die Integrität von IT-Systemen.

Darüber hinaus ist der mit dem vorliegenden Gesetzentwurf vorgesehene Einsatz im Rahmen der Gefahrenabwehr nicht zielführend und praktikabel. Die Zeitkritikalität bei der Gefahrenabwehr schließt den Einsatz von Trojanern aus, da dafür langwierige und aufwendige Vorarbeiten erforderlich sind. Es dürfe daher zweifelhaft sein, ob mit der geplanten Befugnis überhaupt ein Beitrag zur Gefahrenabwehr erreicht werden kann.

Im Kontext mit dem hier geplanten Trojanereinsatz wird eco schließlich eine Gesamtschau mehrerer Überwachungsmaßnahmen aus anderen, aktuellen Gesetzesvorhaben vornehmen, um aufzuzeigen, welches Ausmaß an Überwachungsmaßnahmen alsbald zu befürchten steht.

Zu den vorgeschlagenen Regelungen

§ 27d BPolGE - Telekommunikationsüberwachung

Keine realistischen Anwendungsszenarien

Angesichts des notwendigen Aufwands zur Infiltration der Geräte von Zielpersonen und der dafür erforderlichen Zeit (Erforschung des Geräts und dessen Software, Aufspüren von Lücken, Aufspielen der Trojaner-Software, Funktionstest) ist im Bereich der Gefahrenabwehr kaum ein Anwendungsfall denkbar, wo alle eben genannten Schritte durchgeführt werden konnten und eine Gefahrenabwehr dann noch möglich ist.

Ausnützen von Schwachstellen und Lücken

Ein erhebliches Problem beim Einsatz von Trojanern ist der ihm innenwohnende Anreiz zum Offenhalten und Ausnutzen bestehender Schwachstellen und Lücken in verbreiteter Software. Hierdurch ist es vergleichsweise einfach möglich mit Trojanersoftware das IT-System einer Zielperson zu infiltrieren. Die Geheimhaltung solcher Schwachstellen und Lücken gefährdet jedoch in großem Umfang Bürger, Unternehmen und staatliche Einrichtungen. Durch die Geheimhaltung wird eine umgehende Beseitigung von Schwachstellen und Lücken verhindert und hierdurch das Risiko geschaffen, dass Kriminelle durch Ausnützen dieser Lücken

beispielsweise große Botnetze aufbauen oder ausländische Nachrichtendienste diese gegenüber deutschen Bürgern, Unternehmen und dem deutschen Staat zum Ausspähen nutzen können.

Die aktuellen, korrigierten Zahlen des Bundesamtes für Justiz zum Einsatz der gegenwärtigen Trojaner[1] und der entsprechende Zeit-, Personal- und Kostenaufwand bestätigen den Anreiz zum Ausnutzen von Softwarelücken in weitverbreiteter Standardsoftware und Anwendungen.

Unzureichende Kontrolle

Mangels technischer Expertise bzgl. Funktionsweise von Trojanern und Auswirkungen deren Einsatzes bei Bundespolizei und zuständigem Amtsgericht kann dort nicht beurteilt werden, ob der Staatstrojaner im konkreten Einzelfall nur innerhalb des gesetzlich erlaubten Rahmens Kommunikation aufgenommen und ausgeleitet hat. Schäden an oder Beeinträchtigungen von IT-Systemen werden bereits systemmatisch überhaupt nicht erfasst.

Online-Durchsuchung „light“

Gem. § 27d Abs. 3 Nr. 3 BPolGE wird geregelt, dass ab dem Zeitpunkt der Anordnung der Maßnahme die Kommunikation aufgezeichnet werden kann. Dies ermöglicht faktisch eine Online-Durchsuchung auch der zurückliegenden Kommunikation. Denn aus technischer Perspektive ist ein Softwaremodul mit der Fähigkeit zur Durchsuchung gespeicherter Kommunikation funktional identisch mit demjenigen, welches eine zeitlich wie inhaltlich umfassende Online-Durchsuchung des Geräts ermöglicht, vgl. BVerfGE, 120, 274, Rn. 188ff.

Fehlende Einschränkung

Im Gegensatz zu § 100a Abs. 1 S. 1 Nr. 2 StPO (Quellen-TKÜ für Strafverfolgung) fehlt die Einschränkung, dass im Einzelfall eine Tat bzw. hier eine Gefahr besonders schwer wiegen muss. Das Fehlen dieser Einhegung stößt auf verfassungsrechtliche Bedenken, da diese Schranke geradezu dafür vorgesehen ist, um der hohen Eingriffsintensität zu Gunsten der Betroffenen ausgleichend Rechnung zu tragen.

Unbestimmtheit

Den Verweis auf das Telekommunikationsgesetz und die Telekommunikationsüberwachungsverordnung (TKÜV) nach § 27d Abs. 7 S. 2 BPolG erachtet eco als zu unbestimmt. Offen ist zudem, ob für diesen Bereich die zugehörige technische Richtlinie nicht gelten soll, da auf sie nicht ausdrücklich verwiesen wird. Dies sieht eco kritisch, da in der Technischen Richtlinie TKÜV auch längere Umsetzungsfristen für die Unternehmen vorgesehen werden können**.** Das Fehlen

[1] https://www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung_node.html

des Verweises führt zur Unbestimmtheit und folglich gibt es den Unternehmen keine ausreichende Rechtssicherheit.

Zuständigkeit Amtsgericht

Nach Ansicht des eco ist die vorgesehene Zuständigkeit der Amtsgerichte für die Anordnung des verdeckten Eingriffs in IT-Systeme nach § 27d Abs. 2 S. 1 BPolGE i. V. m. § 28 Abs. 4 S. 4 bedenklich. Im Hinblick auf die Eingriffsintensität der Maßnahme erachtet eco zumindest die Zuständigkeit einer Kammer des jeweils örtlich zuständigen Landgerichts in der Besetzung mit drei Berufsrichtern für erforderlich und angemessen. In der praktischen Erfahrung hat sich gezeigt, dass Amtsgerichte Anträge auf Anordnung einer TKÜ-Maßnahme nur im absoluten Ausnahmefall ablehnen, vgl. die öffentlich zugänglichen Zahlen[2] zum Bundesland Berlin.

Kontrolle d. BfDI nach §35f und § 37 BPolGE

Grundsätzlich positiv bewertet eco die vorgegebene Protokollierung nach § 35f BPolGE und die Kontrolle durch den BfDI gem. § 37 BPolGE. Letztere sollte hinsichtlich der Eingriffsintensität des verdeckten Zugriffs auf IT-Systeme nach § 27d Abs. 2 S. 1 BPolGE jährlich stattfinden. Je größer die Eingriffsintensität, desto kürzer müssen die zeitlichen Kontrollabstände sein.

Gesamtbetrachtung aktueller Gesetzgebungsverfahren in diesem Kontext

In mehreren anderen der aktuellen Gesetzesvorhaben sind viele neue Überwachungsmaßnahmen geplant - neu insbesondere in dem Sinne, dass nun auch Messenger und E-Mail Diensteanbieter erfasst werden und der Kreis der Verpflichteten so um ein Vielfaches der bisher betroffenen Unternehmen anwächst. Zu allen im Folgenden genannten Vorhaben hat eco auch Stellung genommen, s. jeweilige Links:

- TKMoGE (BT-Drs. 19/26108): Sieht wieder die Vorratsdatenspeicherung, eine Verpflichtung zur Mitwirkung der TK-Unternehmen bei der Umleitung von Datenverkehren zum Aufspielen von Trojanern, und eine Identifizierungspflicht der Messenger und E-Maildiensteanbieter hinsichtlich deren Nutzern vor, vgl. https://www.eco.de/download/146723/;

- VerfSchGE (BT-Drs. 19/24785): Räumt die Befugnis zum Einsatz von Trojanern für alle deutschen Nachrichtendienste bzgl. aller Arten von TK-Diensten (auch Messenger und E-Maildienste) und Verpflichtung zur Mitwirkung der TK-Unternehmen bei der Umleitung des Datenverkehrs zum Aufspielen von Trojanern vor, vgl. https://www.eco.de/download/140669/;

- IT-SiG 2.0 (BT-Drs. 19/26106): Regelt, dass das BSI grundsätzlich zur Warnung von Herstellern

[2] https://pardok.parlament-berlin.de/starweb/adis/citat/VT/18/DruckSachen/d18-2836.pdf

verpflichtet, wenn der Behörde Lücken bekannt werden. Davon kann abgesehen werden, wenn dem Interessen Dritter entgegenstehen. Die nun neue Begründung (S. 66) zu § 7 Abs. 1a BSIGE stellt klar, dass damit zukünftig das Interesse der zum Trojanereinsatz berechtigten Stellen gemeint ist, also das Geheimhalten solcher Lücken, vgl. https://www.eco.de/download/141055/;

- BNDGE (BT-Drs. 19/26103): Schafft die Befugnis zum Hacking ausländischer TK-Anbieter und Plattformen (So beispielsweise Google, Facebook, Amazon, Apple, usw.) und von Individuen, vgl. https://www.eco.de/download/140744/;

- GE Bestandsdatenauskunft - NetzDG (BT-Drs. 19/25294): Regelt die Verpflichtung zur Bestandsdatensammlung für alle TK-Anbieter und eine Meldepflicht sozialer Netzwerke von Verdachtsfällen an das BKA, vgl. https://www.eco.de/download/141072/

Nach Auffassung des eco wird allein durch diese noch nicht einmal abschließende Aufzählung deutlich, dass der deutsche Gesetzgeber das Maß zwischen Überwachung - welche auf das absolut notwendige begrenzt sein muss - und den Rechten der betroffenen TK-Anbieter und deren Kunden, den Bürgern, völlig aus den Augen verloren. Die TK-Anbieter selbst sind wiederrum ihren Kunden zum Schutz von deren Daten verpflichtet und werden auch hier immer mehr in Anspruch genommen.

Die schiere Anzahl der vorstehenden Überwachungsmaßnahmen weckt mehr als berechtigte Zweifel an einer Angemessenheit der Vorhaben.