Gesattelte Staatstrojaner

Neue Schnüffelwerkzeuge für Geheimdienste

Die große Koalition hat schier alle Sicherheitsbehörden mit der Lizenz zum Hacken von Smartphones und Computern ausgestattet und so die Grenzen des Rechtsstaats verschoben. Das ist schlecht für die IT-Security; für die Gefahrenabwehr oder die Strafverfolgung bringt es wenig.

Von Stefan Krempl

Dutzende neue Überwachungsgesetze hat die Politik nach dem 11. September 2001 in Deutschland geschaffen und die Befugnisse der Sicherheitsbehörden massiv ausgeweitet. Die „GroKo“ gab auf den letzten Metern der aktuellen Legislaturperiode noch einmal Gas und rüstete mit einem Gesetzesbeschluss im Bundestag im Juni alle 19 Geheimdienste von Bund und Ländern mit der Lizenz zum Einsatz von Staatstrojanern aus. Dabei hatten Experten bei einer Anhörung gewarnt, der Gesetzgeber laufe so „sehenden Auges in die Verfassungswidrigkeit“.

Mit dieser Anpassung des Verfassungsschutzrechts dürfen das Bundesamt für Verfassungsschutz (BfV), der Bundesnachrichtendienst (BND), der Militärische Abschirmdienst (MAD) und die Verfassungsschutzämter der Länder mithilfe der Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) Chats via WhatsApp, Signal, Threema & Co. sowie Internet-Telefonate und Video-Calls mitschneiden. Dafür müssen sie in der Regel Schwachstellen in IT-Systemen ausnutzen, was die Gerätesicherheit für alle gefährdet und Cyberkriminellen sowie ausländischen Geheimdiensten ebenfalls Türen öffnen könnte.

Mit der Mehrheit von CDU/CSU und SPD gegen alle übrigen Oppositionsparteien stimmte der Bundestag für die „Quellen-TKÜ plus“. So dürfen die weit im Vorfeld konkreter Gefahren agierenden Agenten nicht nur die laufende Kommunikation etwa direkt am gehackten Mobiltelefon abgreifen, bevor sie ver- oder nachdem sie entschlüsselt wurde, sondern auch gespeicherte Chats und Mails. Die Grenze zur heimlichen Online-Durchsuchung, die ein Stöbern in Datenbergen ermöglicht und einen besonders tiefen Grundrechtseingriff darstellt, wird so noch fließender.

Manipulation durch Geheimdienste

Neu ist eine Klausel, die es den Behörden einfacher machen soll, Nutzer auszuspionieren: Anbieter von Telekommunikationsdiensten müssen die „berechtigten Stellen“ dabei unterstützen, „technische Mittel“ wie Staatstrojaner „einzubringen“ und die Kommunikation an sie umzuleiten. Juristen und Provider beklagen hier ein massives Missbrauchspotenzial: Damit werde nicht nur eine Kopie der Kommunikation ausgeleitet, sondern gezielt die Manipulation der Daten durch die Geheimdienste ermöglicht.

Schwarz-Rot stellte wegen der Kritik noch klar, dass diese Pflicht nur öffentliche Telekommunikationsanbieter trifft. Betreiber von App-Stores, Messengern und Mail-Diensten bleiben außen vor. Etwaige Schlüssel müssen nicht herausgegeben werden.

Lange Tradition

Auch Strafverfolger wie die Polizeien von Bund und Ländern dürfen prinzipiell bereits im Rahmen ihrer alltäglichen Arbeit verschlüsselte Internet-Telefonate und Chats live überwachen. Eine entsprechende Basis für die Quellen-TKÜ schuf das Parlament 2017 über eine Novelle der Strafprozessordnung (StPO) mit den Stimmen von Schwarz-Rot. Als Voraussetzung dafür gilt der breite Deliktkatalog aus Paragraf 100a StPO. Die Liste fängt mit Mord und Totschlag an und reicht über Steuerdelikte und Computerbetrug bis zum Verleiten von Flüchtlingen zum Stellen eines missbräuchlichen Asylantrags.

Die Ermittler erhielten zudem die Befugnis, beim Verdacht auf „besonders schwere Straftaten“ heimlich Festplatten und Rechner auszuspähen. Diese Klausel für Online-Durchsuchungen ist an den strikteren Paragrafen 100c StPO gekoppelt, der den großen Lauschangriff regelt. Unklar blieb, wie bei den Maßnahmen das vom Bundesverfassungsgericht im Streit um Computerwanzen 2008 entwickelte Recht auf Vertraulichkeit und Integrität von IT-Systemen in der Praxis gewahrt werden soll. Die Opposition sprach von

Bild: Wolfgang Kumm/dpa

Die von Innenminister Horst Seehofer (rechts) initiierten Gesetzespakete ermächtigen Verfassungsschutz-Chef Thomas Haldenwang (links), IT-Sicherheitslücken auszunutzen und Spionagesoftware zur Überwachung auf PCs und Smartphones einzuschleusen.

einem der „invasivsten Überwachungsgesetze der letzten Jahre“. Gegen die Novelle laufen Verfassungsbeschwerden.

Kompetenzgerangel

Schwarz-Rot wollte auch der Bundespolizei den Bundestrojaner in die Hand drücken. Ein Entwurf von CDU/CSU und SPD sah vor, dass die Behörde künftig Telekommunikation auch präventiv überwachen können sollte, etwa „zur Abwehr einer dringenden Gefahr“. Dies hätte Fälle ohne konkreten Anfangsverdacht und die Quellen-TKÜ eingeschlossen. Der Koalition zufolge sollte die Bundespolizei damit vor allem lebensgefährdende Schleusungen sowie gefährliche Eingriffe in den See-, Luft- oder Bahnverkehr in den Blick nehmen.

Laut Schwarz-Rot hätten sämtliche Diensteanbieter es der Bundespolizei ermöglichen müssen, „die zur Auskunftserteilung erforderlichen Daten“ auf einem noch zu bestimmenden Weg „unverzüglich zu übermitteln“. Die Mitwirkungspflicht wäre hier sogar noch größer gewesen als bei den Geheimdiensten.

Im Unterschied zum Geheimdienstgesetz verweigerte der Bundesrat Ende Juni jedoch die Zustimmung zum vom Bundestag beschlossenen Entwurf. Ein Dorn im Auge war der Länderkammer die vorgesehene Ausweitung des Einsatzbereichs der Bundespolizei bei länderübergreifenden Delikten wie Aufbrüchen von Ticketautomaten. Niedersachsens Innenminister Boris Pistorius (SPD) betonte, dass diese Einschnitte in die Kompetenzen der Länderpolizeien einen „dunklen Schatten“ würfen.

Seltene Einsätze

Wie oft Staatstrojaner zur Strafverfolgung genutzt werden, machte das Bundesamt für Justiz (BfJ) im Dezember 2020 erstmals mit Statistiken für 2019 publik. Anfangs war von 578 Anordnungen für die Quellen-TKÜ die Rede, von denen 368 in die Tat umgesetzt worden seien. Zusätzlich wies das BfJ 20 Verfahren aus, in denen eine Online-Durchsuchung angeordnet worden war. Davon konnten 12 tatsächlich durchgeführt werden.

Doch es tauchten Zweifel an den Zahlen auf. Mehrere Länder signalisierten, in den Bögen Felder falsch angekreuzt zu haben. Letztlich korrigierte das BfJ die Angaben drastisch nach unten: Demnach wurden Staatstrojaner nur insgesamt 15-mal verwendet, davon dreimal zur Quellen-TKÜ. Sebastian Fiedler vom Bund deutscher Kriminalbeamter hob hervor, dass die komplizierte Form der Überwachung in der Praxis nur selten gelinge. Für die deutsche Polizei sei die Quellen-TKÜ „kein Alltagswerkzeug“.

Bild: ZITiS/YouTube

Der Bund greift nicht nur auf Spionageprogramme von privaten Firmen zurück, sondern brütet auch eigene Staatstrojaner aus in der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS).

Ähnlich sieht es beim BKA aus: Der Fraktionsvize der Grünen, Konstantin von Notz, erklärte im Februar mit Verweis auf eine Regierungsantwort, dass die Behörde zwischen 2017 und 2020 in keinem einzigen abgeschlossenen Ermittlungsverfahren oder Gefahrenabwehrvorgang den Bundestrojaner angewandt habe.

Made in Germany

Lange tat sich das BKA schwer mit der Entwicklung und Beschaffung geeigneter Software. Der von ihm zunächst in Eigenregie für 5,77 Millionen Euro gebaute Bundestrojaner taugte anfangs nur für das Abfangen laufender Kommunikation auf stationären Rechnern. Eine leistungsstärkere Version für Online-Durchsuchungen war lange in der Mache. Parallel beschaffte sich das BKA etwa die Spähsoftware FinSpy des umstrittenen Münchner Unternehmens FinFisher (Gamma Group). Mittlerweile hat es drei Software-Pakete zur Verfügung und dafür Dutzende Millionen Euro ausgegeben.

2018 hatte ein BKA-Vertreter im Innenausschuss des Bundestags auf dem Markt für Überwachungssoftware eine „dramatisch zugespitzte“ Lage ausgemacht und auf einen „Konzentrationsprozess“ verwiesen. Aktenkundig ist, dass die hessische Firma DigiTask, die den Bayerntrojaner programmierte, von der Leipziger Firma ipoque übernommen wurde, die zum Konzern Rohde & Schwarz gehört. Der kooperiert wiederum eng mit der staatlichen Hackerbehörde „Zentrale Stelle für Informationstechnik im Sicherheitsbereich“ (ZITiS), die seit einiger Zeit an Staatstrojanern für Sicherheitsbehörden werkelt.

Staatliche Eigenentwicklung auf diesem Gebiet hält das Bundesinnenministerium für unverzichtbar, um Abhängigkeiten von Herstellern und Dienstleistern aus dem Nicht-EU-Ausland zu verringern und „das Einhalten gesetzlicher Vorgaben und der korrespondierenden ethischen Werte sicherzustellen“. Ferner müsse es möglich sein, dass sich die Bedarfsträger „moderner Verfahren und Entwicklungen aus globalen Lieferketten bedienen“. Um „gesichert und selbstbestimmt“ Staatstrojaner beschaffen zu können, baue die ZITiS die Kompetenz auf, „zu beraten und Produkte evaluieren zu können“.

Dass eine neue Regierung nach der Bundestagswahl Befugnisse im großen Stil zurücknimmt, ist kaum zu erwarten. Die CDU will die Voraussetzungen für den Einsatz von Staatstrojanern bei Quellen-TKÜ und Online-Durchsuchung „bundesweit anpassen“, sodass diese Instrumente „rechtssicher und effektiv eingesetzt werden können“. Bund und Länder sollen dafür eine gemeinsame Software erhalten. Die SPD hält an dem Werkzeug fest. Der Grünen-Vorstand machte sich in einem Entwurf fürs Wahlprogramm dafür stark, dass Ermittler „technische Geräte anhand einer rechtsstaatlich ausgestalteten Quellen-TKÜ zielgerichtet“ infiltrieren können sollten. Die Parteibasis lehnte dies aber ab.

Klar gegen Staatstrojaner sind die FDP und die Linke. Die AfD spricht sich in ihrem Parteiprogramm zwar dafür aus, dass „Datenschutz kein Täterschutz“ sein dürfe, stimmte im Bundestag aber ebenfalls gegen eine Ausweitung der Befugnisse des Verfassungsschutzes. Die Partei wehrte sich im Frühjahr juristisch gegen bundesweite Beobachtungen aufgrund des Verdachts rechtsextremistischer Aktivitäten. *(hag@ct.de)* c't