Quellen-TKÜ – praktisch irrelevant

Wenn Telefonate, E-Mails und Chats verschlüsselt sind, soll die Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) helfen. In der Praxis spielt sie bisher jedoch kaum eine Rolle. Es fehlt an passenden Trojanern und es ist schwierig, sie auf dem Zielgerät zu platzieren. *Von Christian Rath*

Immer mehr Kommunikation ist und wird heute verschlüsselt. Klassische Telekommunikationsüberwachung, bei der die Inhalte auf dem Übertragungsweg ausgeleitet werden, ist dann nicht mehr möglich. Hier kann nur noch die Quellen-TKÜ eingesetzt werden. Bei ihr platziert die Polizei eine Spähsoftware auf dem Computer oder dem Smartphone der Zielperson. Dieser Staatstrojaner fängt die Telekommunikation an der Quelle ab – bevor sie verschlüsselt wird. So kann die Polizei auch auf verschlüsselte Telefonate, E-Mails und SMS zugreifen. Bei der Überwachung von Messengerdiensten muss der Staats-Trojaner sogar Inhalte erfassen, die bereits abgespeichert sind.

Die Quellen-TKÜ in Deutschland hat eine wechselhafte Geschichte. Lange Zeit wurde sie ohne spezielle Rechtsgrundlage auf den klassischen Abhör-Paragrafen 100a der Strafprozessordnung gestützt. 2007 wurde der Einsatz von Staatstrojanern öffentlich bekannt – als Online-Durchsuchung (mit Zugriff auf die Festplatte) und als Quellen-TKÜ (mit Zugriff auf die laufende Kommunikation). 2008 billigte das Bundesverfassungsgericht die Quellen-TKÜ, sofern es rechtliche und technische Vorkehrungen gibt, die den Zugriff des Trojaner auf die laufende Kommunikation beschränken. Ab nun wurde zwar über eine spezielle Rechtsgrundlage diskutiert, doch Polizei, Staatsanwaltschaften und Gerichte nutzten weiter § 100a StPO.

Doch als der Chaos Computer Club 2011 nachwies, dass für die Quellen-TKÜ eingesetzte Staatstrojaner viel mehr konnten, als sie durften, wurden die Maßnahmen sofort gestoppt. Es gab nun jahrelang keine Quellen-TKÜs mehr. Erst 2016 präsentierte das Bundeskriminalamt (BKA) einen selbst programmierten Trojaner, der die Karlsruher Vorgaben einhielt. 2017 schuf die große Koalition dann auch eine spezielle Rechtsgrundlage in § 100a Abs. 1 Satz 2 und 3 StPO. Für präventiv-polizeiliche Zwecke enthielten das BKA-Gesetz und die meisten Länder-Polizeigesetze schon länger Grundlagen für Quellen-TKÜ-Maßnahmen.

Mit der neuen StPO-Regelung wurde 2017 auch eine Berichtspflicht eingeführt. In der jährlichen TKÜ-Statistik des Bundesamts für Justiz wird die Quellen-TKÜ nun separat dargestellt, erstmals für das Jahr 2019. Die Zahlen für 2020 werden erst Anfang kommenden Jahres veröffentlicht. Die Statistik für 2019 wies in Bund und Ländern genau 31 strafprozessuale Quellen-TKÜ-Anordnungen aus, nur ganze drei Mal wurde die angeordnete Quellen-TKÜ auch durchgeführt. In der Praxis spielt die Quellen-TKÜ also fast keine Rolle. Das hat verschiedene Gründe.

Erstes Problem ist der Mangel an geeigneten Trojanern. Die 2016 vorgestellte erste BKA-Eigenproduktion konnte nur Computer mit den Betriebssystemen Windows 7 und Windows 8 infiltrieren. Damals war aber schon Windows 10 auf dem Markt. Und der Einsatz auf Mobiltelefonen war noch gar nicht möglich, obwohl bei Smartphones eigentlich der Hauptbedarf bestand. Inzwischen steht dem BKA auch ein zweiter selbst programmierter Trojaner zur Verfügung, über den das BKA aber keine Auskunft gibt. Möglicherweise soll die Geheimniskrämerei nur verdecken, wie wenig operative Fähigkeiten die Polizei-Trojaner haben. Immerhin gibt es seit 2017 auch die „Zentrale Stelle für Informationstechnik im Sicherheitsbereich" (ZITiS) in München. Soweit ersichtlich hat sie aber noch keinen für die Polizei brauchbaren Trojaner entwickelt. Schon 2013 beschaffte das BKA einen kommerziellen Trojaner der deutsch-britischen Firma FinFisher. Laut Spiegel dauerte es fünf Jahre, bis er an das deutsche Recht angepasst und damit einsatzfähig war. 2019/20 beschaffte das BKA auch die Pegasus-Software der israelischen Firma NSO. Genutzt wird eine Version mit beschränktem Funktionsumfang. Doch neben der Justierung für das deutsche Recht, muss die Polizei vor jedem Trojaner-Einsatz auch herausfinden, welches Gerät die Zielperson nutzt und welches Betriebssystem in welcher Version dort installiert ist. Hierauf muss der jeweilige Trojaner dann aufwendig abgestimmt werden.

Zweites Problem ist das Aufspielen der Spähsoftware auf den Computer oder das Smartphone der Zielperson. Hierfür gibt es vor allem fünf Methoden. Das heimliche Eindringen in die Wohnung ist bisher strafprozessual nicht erlaubt. Die Einbruch-Lösung scheidet in Deutschland also aus. Die Polizei versucht daher überwiegend durch List Zugriff auf das Smartphone oder den Laptop zu bekommen, etwa bei einer Beschlagnahme oder einer fingierten Verkehrs- oder Zollkontrolle. Hier ist die Zielperson nach Rückgabe des Geräts aber oft misstrauisch.

Daneben gibt es mehrere Möglichkeiten des Fernzugriffs. Am bekanntesten ist der Versand einer E-Mail mit einem präparierten Anhang an die Zielperson. Bei vorsichtigen Zielpersonen sind oft mehrere Versuche mit jeweils auf die Person angepassten E-Mail-Anhängen nötig. Ähnliches gilt für das Zusenden eines Links, der auf eine „verseuchte", das heißt präparierte, Webseite führt. Der Pegasus-Trojaner kann das Zielgerät sogar infiltrieren, ohne dass der Nutzer auf einen Anhang oder einen Link klicken muss (zero click exploit). Dabei werden jeweils Schwachstellen der Hard- oder Software genutzt, die die Sicherheitsbehörden von spezialisierten Hackern aufkaufen.

Die Nutzung solcher IT-Schwachstellen ist politisch allerdings hochumstritten, da sie auch von Straftätern genutzt werden könnten. Das Bundesverfassungsgericht entschied im Juli 2021, dass der Staat zwar eine Schutzpflicht habe, wenn er von bisher unbekannten Schwachstellen erfahre. Die Sicherheitsbehörden müssten aber nicht sofort den Hersteller der betroffenen Hard- oder Software informieren, sondern können die Schwachstelle zunächst nutzen – wenn sie Chancen und Risiken nach festen Regeln abgewogen haben. Die Bundesregierung hat im September eine Cybersicherheitsstrategie beschlossen und sich dabei zum „verantwortungsvollen Umgang" mit IT-Schwachstellen bekannt.

Drittes Problem ist das Entdeckungsrisiko. Antiviren-Software wie Kaspersky versucht auch Schutz gegen Trojaner zu geben. Außerdem kann das Aufspielen des Trojaners zu unbeabsichtigtem irregulärem Verhalten des Geräts führen. Wenn die Zielperson so auf den staatlichen Überwachungsversuch aufmerksam wird, muss die Polizei nicht nur auf neue Erkenntnisse verzichten, sie hat sogar Nachteile, weil die Zielperson nun von den Ermittlungen weiß und gewarnt ist.

Aus all diesen Gründen setzen Ermittler die Quellen-TKÜ nur äußerst selten ein. Selbst das BKA sagt, die Quellen-TKÜ sei „keine Alternative zur klassischen TKÜ". Und so sieht das auch die Polizei in der Praxis. In den letzten zehn Jahren gab es jährlich stets rund 18.000 Anordnungen konventioneller TKÜ.

Dr. Christian Rath
ist rechtspolitischer Korrespondent u. a. der „taz", der „Badischen Zeitung" und des „RedaktionsNetzwerks Deutschland".