PB.Z-01-747-4 Kapitel 5: Zusammen leben

Antragsteller*in: BAG Digitales und Medien
Beschlussdatum: 14.04.2021

Änderungsantrag zu PB.Z-01

Von Zeile 746 bis 751:
müssen auf valider Empirie beruhen und verfassungsrechtliche Vorgaben zwingend beachten. ~~Statt pauschaler, anlassloser Vorratsdatenspeicherung und genereller Backdoors für Sicherheitsbehörden oder Staatstrojaner für Geheimdienste wollen wir es der Polizei ermöglichen, technische Geräte anhand einer rechtsstaatlich ausgestalteten Quellen-TKÜ zielgerichtet zu infiltrieren. Zudem soll eine Meldepflicht für Sicherheitslücken eingeführt werden.~~Technische Instrumente, die Dritte in ihrer Sicherheit gefährden, lehnen wir ab. Daher sprechen wir uns gegen Vorratsdatenspeicherung, Verschlüsselungsschwächung und das Sammeln von Sicherheitslücken aus. Wo Befugnisse mit Eingriffen in die Grundrechte erforderlich sind, dürfen diese neben der notwendigen Verhältnismäßigkeit auch nie mittelbar oder unmittelbar auf die Allgemeinheit oder nicht Betroffene wirken. Stattdessen wollen wir die Sicherheitsbehörden technisch und personell besser für moderne Verbrechensbekämpfung ausstatten. Die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) befasst sich u.a. im Auftrag der Polizeien und Nachrichtendienste des Bundes mit diesen hochsensiblen Themen, wir fordern daher die Abschaffung der ZITiS.

Begründung

Der ursprüngliche Antragsentwurf ist so formuliert, dass derzeit die Infiltration von technischen Geräten für eine "rechtsstaatlich ausgestaltete Quellen-TKÜ" ermöglicht werden soll.

Der Wunsch, hier den Interessen der Sicherheitsbehörden entgegen zu kommen, ist nachvollziehbar, schließlich wird in einer zunehmend digitalisierten Welt die Gewinnung von Ermittlungserkenntnissen mit traditionellen Methoden schwieriger. Doch eine Quellen-TKÜ muss derzeit überhaupt nicht ermöglicht werden, da die Strafprozessordnung 2017 geändert wurde, um Quellen-TKÜ explizit mit zu regeln, nachdem sie – juristisch sehr umstritten – zuvor auch schon durch die Rechtsgrundlage der klassischen TKÜ angewandt wurde [1]. Die Quellen-TKÜ kann nun also wie die klassische Telekommunikationsüberwachung eingesetzt werden, erfordert aber eine völlig andere Methode.

Da mit ihr die Ende-zu-Ende-Verschlüsselung moderner Kommunikation umgangen wird, funktioniert sie nur, indem auf dem digitalen Endgerät der Betroffenen, ohne deren Kenntnis, Software zur Überwachung integriert wird, die die Kommunikation vor der Ver- bzw. nach der Entschlüsselung zu einem Server der Ermittlungsbehörden (bzw. deren Dienstleister) ausleitet. Diese Software hat dabei gezwungenermaßen die gleichen Zugriffsrechte und weitgehend identische Funktionalität, wie eine Überwachungssoftware zur sogenannten "Online-Durchsuchung" oder aber Schadsoftware Krimineller. Die Kompromittierung des IT-Systems der Betroffenen ist aus Perspektive der IT-Sicherheit in allen Fällen gleichwertig und ermöglicht durch zu

erwartende Schwachstellen in der Überwachungssoftware womöglich auch den Zugriff Unbefugter.

Die Qualität dieser schweren Eingriffstiefe lässt sich dabei kaum durch eine bessere juristische Ausgestaltung heilen, sondern besteht bereits durch die grundsätzliche Kompromittierung der IT-Sicherheit des jeweiligen Endgeräts. Denn Software zur "Onlinedurchsuchung" oder aber "Quellen-TKÜ" sind aus Sicht der Betroffenen natürlich Schadprogramme, die entweder durch IT-Sicherheitsschwachstellen auf die Endgeräte der Betroffenen eingespielt werden – die wir aus guten Gründen im Entwurf zu schließen versuchen – oder aber durch geheimdienstähnliche Manipulation der Endgeräte der Betroffenen. Also indem man sich heimlich Zugang zu diesen Endgeräten verschafft und diese Software dann aufspielt. Beide Vorgehensweisen sind technisch schwierig umzusetzen und selten von Erfolg gekrönt.

Gleichzeitig stellt diese mit diesem Werkzeug verbundene Infrastruktur natürlich auch ein komplexes IT-System dar, dessen technische Absicherung in der Praxis nicht immer allgemeinen IT-Sicherheitsstandards genügt. Den unberechtigten Zugriff Unberechtigter zu verhindern, stellt ein nicht zu unterschätzendes Problem dar. Derartige Gefährdungen lassen sich nicht allein durch eine "rechtsstaatliche Ausgestaltung" zuverlässig abwenden.

In der Praxis stellt sich daher heraus, dass Ermittlungsbehörden die sogenannte Quellen-TKÜ nur in verschwindend geringem Maße einsetzen – und dass diese häufig gar nicht richtig verstanden wird. In der im Dezember 2020 vorgestellten Statistik des Bundesjustizministeriums für 2019 wurden 578 angeordnete und 368 durchgeführte Maßnahmen der Quellen-TKÜ ausgewiesen [2]. Wenig später stellte sich jedoch heraus, dass der Fragebogen zur Datenabfrage nicht immer richtig verstanden wurde. Im Februar 2021 wurde dementsprechend klar: Nur drei von 31 angeordneten Maßnahmen zur Quellen-TKÜ wurden 2019 durchgeführt. "'Diese hoch komplizierte Form der Überwachung gelingt in der Praxis leider zu selten. Das ist gemeinhin bekannt.' Für die deutsche Polizei sei die Quellen-TKÜ 'kein Alltags-Werkzeug'" [3].

Fazit: Die Quellen-TKÜ ist in ihrer derzeitigen technischen Ausgestaltung und den daraus erwachsenden Risiken für IT-Sicherheit, sowie dem entstehenden Aufwand und den geringen Erfolgsaussichten nicht von der sogenannten Onlinedurchsuchung durch das gemeinhin "Staatstrojaner" genannte Werkzeug nicht zu unterscheiden. Sie hat keine praktische Bedeutung und lenkt die Ressourcen von IT-Know-How bei unserer Polizei somit in unverhältnismäßig aufwändige Ermittlungsverfahren. Es ist sehr viel sinnvoller, diese Ressourcen in die Auswertung leichter zu erlangender Ermittlungskenntnisse aus digitalen Quellen zu lenken und mit besserer Ausbildung, besserer Bezahlung und besserer technischer statt juristischer Ausstattung die Polizeiarbeit unterstützen.

[1] https://netzpolitik.org/2017/staatstrojaner-bundestag-beschliesst-diese-woche-das-krasseste-ueberwachungsgesetz-der-legislaturperiode/

[2] https://netzpolitik.org/2020/justizstatistik-2019-die-polizei-setzt-taeglich-staatstrojaner-ein-update/

[3] https://www.tagesschau.de/investigativ/ndr-wdr/polizei-staatstrojaner-kriminelle-101.html

Weiterführende Informationen: https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf

Zur ZITiS: Die ZITiS haben wir schon 2017 klar abgelehnt und sollten dies auch weiter vertreten. (u.a. https://www.gruene-bundestag.de/parlament/bundestagsreden/zentrale-stelle-fuer-informationstechnik-im-sicherheitsbereich)