VERBAND DER INTERNETWIRTSCHAFT E.V.

Eckpunkte zum Gesetzesentwurf zur Anpassung des Verfassungsschutzrechts (BT-Drs.: 19/24785)

Berlin, 11.05.2021

Mit dem Gesetzesentwurf soll den deutschen Nachrichtendiensten das Recht zur Quellen-TKÜ und zur Online-Durchsuchung von bestimmten, zurückliegenden Kommunikationsdaten eingeräumt werden. eco bewertet den Gesetzentwurf kritisch und sieht erheblichen Änderungsbedarf. Diese Ermittlungsmethoden schwächen die IT-Sicherheit, die Integrität von IT-Infrastrukturen und Vertrauenswürdigkeit von Kommunikation. eco erkennt an, dass es ein berechtigtes Interesse gibt, den Herausforderungen im Bereich des internationalen Terrorismus, des Rechtsterrorismus, und organisierter Kriminalität wirksam entgegenzutreten. Gleichwohl stehen nach Auffassung des eco stehen die zu erzielenden Ermittlungsergebnisse außer Verhältnis zu den vorgenannten Schwächungen und daraus resultierenden Gefährdungen für Bürger und Bürgerinnen, die Wirtschaft und nicht zuletzt den Staat selbst.

Nachfolgend möchten wir unseren zentralen Kritikpunkte noch einmal darlegen. Ergänzend weisen wir auf unsere ausführliche Stellungnahme hin.

I. Erweiterung der Befugnisse zur Online-Durchsuchung für alle 19 Geheimdienste

eco lehnt die Erweiterung der Befugnisse zur Online-Durchsuchung strikt ab. Entgegen allen öffentlichen Bekundungen sollen mit dem vorliegenden Gesetzentwurf zukünftig allen deutschen Nachrichtendiensten gem. § 2 Absatz 1 S. 1 Nr. 4 G10-Gesetz-E i. V. m. § 11 Abs. 1a S. 1 G10-Gesetz-E zur Online-Durchsuchung berechtigt werden. Aus technischer Perspektive besteht hinsichtlich der eingesetzten Trojaner-Software kein Unterschied bzgl. deren Ausforschungsfähigkeit, ob diese eine uneingeschränkte Online-Durchsuchung ermöglicht oder wie hier vorgesehen auf einen bestimmten Zeitraum sowie auf ruhende Kommunikation bezogen erfolgt. Zur Veranschaulichung: Am 10. Oktober wird der Einsatz des Trojaners gegenüber Person A angeordnet, am 17. Oktober gelingt die Infiltration des technischen Systems von A mit der Trojaner-Software. Der Trojaner soll dann die auf die zurückliegende und damit ruhende Kommunikation ab 10. Oktober zugreifen und auslesen dürfen. Technisch gesehen ist dabei jede Funktion, welche Zugriff auf ruhende Daten nimmt, grundsätzlich geeignet, auf alle älteren Daten im infizierten IT-System der Zielperson zuzugreifen, unabhängig davon ob es sich Kommunikations- oder andere Daten handelt.

II. Schwächung der IT-Sicherheit und Integrität (Ausnutzen v. Lücken)

Eine „Datenerhebung durch Eingriff in die informationstechnischen Systeme“ wird, wenn diese durch das Ausnutzen von Sicherheitslücken durchgeführt werden soll, von eco kritisch bewertet. Damit die IT-Sicherheit insgesamt gestärkt wird, müssen festgestellte Schwachstellen vielmehr unverzüglich gemeldet und beseitigt werden. Online-Durchsuchung und Quellen-TKÜ führen zu einer Schwächung der Sicherheit und der Integrität von IT-Systemen. Beiden Ermittlungsinstrumenten ist gemein, dass sie am einfachsten und besten zu nutzen sind, wenn sie durch die

Ausnutzung Lücken in handelsüblicher und weit verbreiteter Software (Betriebssysteme oder Standardbürosoftware) oder auf dem System des betroffenen Nutzers aufgebracht werden. Das verstärkt den Anreiz der Sicherheitsbehörden, solche Sicherheitslücken geheim zu halten und nicht offenzulegen. Zu Gunsten von Ermittlungen gegen eine einzelne Person Schwachstellen und Lücken offen zu halten, bedeutet für Millionen von privaten, gewerblichen und staatlichen Nutzern hierzulande Gefahren für deren Privatsphäre, deren Eigentum, mittelbar auch deren Vermögen, da auch Kriminelle sie nutzen können oder darüber gefährliche Botnetze aufgebaut werden. Hinzu kommt, dass die Fähigkeiten bzw. Reichweite von Staatstrojanern beim Durchsuchen von IT-Systemen mangels Dokumentationspflichten und Expertenwissen weder durch die Geheimdienste noch durch Gerichte oder die vorhandenen Aufsichtsgremien kontrolliert werden können.

III. Besonders intensiver Eingriff durch „Umleitung“

eco lehnt die Regelung nach § 2 Abs. 1a S. 1, Nr. 4 G10-Gesetz-E ab. Denn mit dem Tatbestandsmerkmal „Umleitung“ wird eine Vielzahl an rechtlichen und prozeduralen Fragen aufgeworfen. Die Anbieter, die geschäftsmäßig Telekommunikationsdienste erbringen oder diejenigen, die an der Erbringung solcher Dienste mitwirken, sollen nunmehr aktiv die Nachrichtendienste bei der Infiltration der Endgeräte Ihrer Kunden unterstützen. Die Datenverkehre der Zielperson sollen vom jeweiligen Anbieter an eine Schnittstelle des ausführenden Nachrichtendienstes umgeleitet und nach Aufspielen des Trojaners wieder durch den TK-Anbieter an die Zielperson zurückgeleitet werden. Dadurch soll eine Quellen-TKÜ und Online-Durchsuchung zeitnah und durch die Ausnutzung des Vertrauens der Kunden in scheinbar vertrauenswürdige Quellen ermöglicht werden. Zu bedenken ist ferner, dass mit dem neuen Telekommunikationsgesetzes (TKG) die Anzahl der grundsätzlich zur Unterstützung verpflichteten Unternehmen massiv ansteigen. Zukünftig werden dann auch Anbieter von E-Mail-, Messaging-, und VoIP-Dienste in die Verpflichtungen einbezogen. eco erachtet die damit verbundene qualitative und quantitative Ausdehnung auf diese genannten Dienste als zu weitreichend und lehnt diese ab.

Nach unserem Verständnis will der Gesetzgeber mit der Regelung in § 2 Abs. 1a S. 1 Nr. 4 G10-Gesetz-E die Befugnis zur Veränderung der betroffenen Datenströme schaffen. Damit würde die Vorschrift sowohl die inhaltliche Veränderung von Daten als auch ein Hinzufügen oder Unterdrücken von Daten ermöglichen. Unabhängig von der Frage, ob derartige Eingriffe überhaupt durch die Beschränkungsmöglichkeit des Art. 10 GG gedeckt sein können, sind solche Maßnahmen jedenfalls geeignet, das Vertrauen in die Kommunikation einschließlich aller abgerufenen Informationen massiv und dauerhaft zu untergraben. eco bewertet daher eine solche Regelung äußerst kritisch und lehnt insbesondere eine Veränderung und Manipulation der Kommunikation sowie deren Unterdrückung entschieden ab. Der gegenwärtige Wortlaut dieser Norm schließt eine Anwendung der Norm durch die Nachrichtendienste zur Veränderung und weitergehender Manipulation in seiner aktuellen Fassung nicht explizit aus. Dementsprechend muss durch den Gesetzgeber ausdrücklich klargestellt werden, dass eine Veränderung von Kommunikation von der Regelung des § 2 Abs. 1a G10-Gesetz-E nicht umfasst und ausgeschlossen ist.

IV. Erfüllungsaufwand der Wirtschaft

eco erachtet den angebenen, voraussichtlichen Erfüllungsaufwand der Wirtschaft mit 20.000€/Jahr für deutlich zu niedrig angesetzt, da die Befugnis zur Quellen-TKÜ sowohl dem BfV, den Landesämtern für Verfassungsschutz, dem BND und dem MAD eingeräumt werden soll. Die mit dem Gesetz vorgesehenen verdeckten Eingriffe in IT-Systeme setzen Expertenwissen im Bereich der Technik, entsprechendes technisches Equipment und Schulung des Personals voraus. Darüber hinaus sind geeignete Prozeduren und Vorgänge zur Umsetzung erarbeitet sowie Maßnahmen zur bestmöglichen Geheimhaltung der Maßnahmen sind zu etablieren. Dies verursacht weitaus höhere Kosten bei jedem einzelnen Unternehmen und übersteigt damit die angegeben Kosten für die gesamte Wirtschaft. Soweit die Aus- bzw. Umleitung unmittelbar in Echtzeit zu erfolgen hätte, bedarf es zudem einer gesicherten Übertragung, die weitere, erhebliche Kosten und Aufwände verursacht. Zudem ist die Höhe des Erfüllungsaufwandes davon abhängig, ob auf bestehende Infrastrukturen zur Datenspeicherung und -ausleitung zurückgegriffen werden kann. Soweit dies möglich ist, würden die Kosten für ggf. erforderliche Schnittstellen bis zu 100.000 € betragen. Wenn jedoch Daten angefordert werden, die bislang noch nicht in den vorhandenen Systemen erfasst sind und entsprechende Anpassungen vorzunehmen wären, sowie potentiell neue Infrastruktur installiert werden muss, wäre ein Kostenaufwand in mehrfacher Millionenhöhe zu erwarten.

V. Evaluierung

eco ist der Ansicht, dass eine Evaluierung von besonders schweren Grundrechtseingriffen wie der Quellen-TKÜ mindestens alle 2 Jahre verfassungsrechtlich zwingend geboten ist. Im Rahmen einer Evaluierung ist zu prüfen, ob sich die neu implementierten Befugnisse wie bspw. die Quellen-TKÜ als geeignet erwiesen haben, ob sie zum Zeitpunkt der Evaluierung weiter erforderlich sind, oder ob zum Zeitpunkt der Evaluierung nicht bereits mildere Mittel mit gleicher Wirksamkeit zur Verfügung stehen. Zudem ist dabei auch zu prüfen, ob diese Befugnisse immer noch als angemessen gelten können, konkret ob durch diese Eingriffe rechtfertigende Ermittlungsergebnisse vorgewiesen werden können. Insbesondere bei verdeckten Maßnahmen wie der Quellen-TKÜ, bei denen Rechtsschutz nur nachträglich möglich ist, und eine Rechtverletzung ggf. nur für die Zukunft unterbleibt, sollte eine Evaluierung unter verfassungsrechtlichen Gesichtspunkten zwingend vorgesehen werden.