Stellungnahme zum Entwurf der Cybersicherheitsstrategie für Deutschland 2021

RSF hat diese Stellungnahme am 16. Juni 2021 im Rahmen der öffentlichen Konsultation des Bundesministeriums des Innern, für Bau und Heimat zum Entwurf der Cybersicherheitsstrategie für Deutschland 2021 über den vorgegebenen Fragebogen eingereicht.

Handlungsfeld 2: „Gemeinsamer Auftrag von Staat und Wirtschaft“

Decken die in diesem Kapitel definierten Ziele die wesentlichen Aspekte und Herausforderungen dieses Handlungsfeldes ab? Eher nein.

Zu 8.2.2 „Die Zusammenarbeit von Staat, Wirtschaft, Wissenschaft und Zivilgesellschaft im Bereich der Cybersicherheit verbessern“

Das Ziel der verbesserten Zusammenarbeit zwischen Staat, Wirtschaft und Zivilgesellschaft begrüßen wir, auch bestehende Initiativen wie den „Dialog für Cybersicherheit“ des BSI nehmen wir positiv wahr. Bei der Einbindung zivilgesellschaftlicher Akteure in Gesetzgebungs- und Strategieprozesse sehen wir jedoch deutlichen Verbesserungsbedarf. Wirksame Beteiligung erfordert angemessene Fristen und die Bereitschaft zur inhaltlichen Auseinandersetzung im erweiterten direkten Dialog. Insbesondere das Kapitel zu Gefahrenabwehr und staatlichen Zugriffsmöglichkeiten zeugt davon, dass gewichtige Kritiken breiter Bündnisse aus Zivilgesellschaft, Wissenschaft und Wirtschaft an Vorschlägen, die bereits seit einigen Jahren Teil der öffentlichen Diskussion sind, keine Berücksichtigung in der Erarbeitung des vorliegenden Entwurfs gefunden haben (Näheres hierzu unter Abschnitt 8.3). Zwischen den angesprochenen Interessen der Sicherheitsbehörden an massiv erweiterten Überwachungs- und Eingriffsbefugnissen und den daraus folgenden Konsequenzen für den Schutz der Grundrechte und der Sicherheit der Bürgerinnen und Bürger scheint keine Abwägung stattgefunden zu haben. Vor diesem Hintergrund sollte klar benannt werden, wie eine wirksame Zusammenarbeit in Zukunft ermöglicht und gestaltet werden soll.

Handlungsfeld 3: „Leistungsfähige und nachhaltige gesamtstaatliche Cybersicherheitsarchitektur“

Decken die in diesem Kapitel definierten Ziele die wesentlichen Aspekte und Herausforderungen dieses Handlungsfeldes ab? Nein.

Definieren die vorangehenden Kapitel die Gewährleistung digitaler Sicherheit noch als gesamtgesellschaftliche Aufgabe, die die Bedarfe verschiedenster Bereiche und Gesellschaftsgruppen abdecken muss, verengt sich in diesem Kapitel der Blick einseitig auf die Interessen der Sicherheitsbehörden, ohne dabei einen angemessenen Ausgleich zwischen staatlichen Aufklärungsinteressen einerseits und der Beeinträchtigung der Bedarfe und Rechte der Bürgerinnen und Bürger andererseits zu suchen. Reporter ohne Grenzen sieht darin eine **erhebliche Gefahr für die Vertrauenswürdigkeit digitaler Kommunikationsmittel und IT-Systeme, auf die sich Medienschaffende und ihre Quellen tagtäglich verlassen.**

Unter dem Titel „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung gewährleisten“ wird die geplante Umsetzung der gleichnamigen Entschließung des EU-Ministerrates skizziert. Der Argumentation der EU-Vorlage folgend wird die „Entwicklung technischer und operativer Lösungen“ und die Erarbeitung gesetzlicher Grundlagen für den Zugriff deutscher Sicherheitsbehörden auf verschlüsselte Kommunikation gefordert. Nur so könne eine effektive Bekämpfung „schwerer und/oder organisierter Kriminalität, Kinderpornographie und Terrorismus“ gewährleistet werden. Dieser Problembeschreibung und der daraus folgenden Zielsetzung widersprechen wir vehement.

Zunächst wird unter Verweis auf die erst in der vergangenen Woche vom Bundestag beschlossene Möglichkeit zum nachrichtendienstlichen Einsatz der Quellen-Telekommunikationsüberwachung zur Überwachung verschlüsselter Nachrichten und Online-Telefonate argumentiert, die auf „Einzelfälle“ beschränkten neuen Befugnisse reichten nicht aus, um der zuvor vage umschriebenen Gefahrenlage gerecht zu werden. Diese Argumentation steht in klarem Widerspruch zu den Aussagen der Vertretenden der Regierungsfraktionen, die eben deren beschränkten und gezielten Einsatz als Kernargument für die Verhältnismäßigkeit dieses äußerst eingriffsintensiven Instruments angeführt haben. Sachverständige aus Rechtswissenschaft, Wirtschaft und Zivilgesellschaft haben die Verfassungsmäßigkeit der (erweiterten) Quellen-TKÜ wiederholt hinterfragt. Dennoch wird hier die Einführung zusätzlicher und noch breiter einsetzbarer Zugriffsmethoden für Polizei und Nachrichtendienste gefordert. Entsprechende Pläne waren bereits 2019 Teil der öffentlichen Diskussion und stießen auf erheblichen Widerstand; mehr als hundert gemeinnützige Organisationen, Firmen, Verbände und Fachleute aus der Wissenschaft sowie Politikschaffende sprachen sich klar gegen einen so tiefen Eingriff in die Grundrechte aus. Diese Bedenken nun zu übergehen widerspricht jeglicher Bekundung des Interesses am gesamtgesellschaftlichen Dialog.

Die Implikationen für die Sicherheit und Vertraulichkeit digitaler Kommunikation sind besorgniserregend, nicht zuletzt angesichts der Bedeutung verschlüsselter Messengerdienste als nutzerfreundliches und breit genutztes Mittel der sicheren Onlinekommunikation, wie Kapitel 8.1.2 ausführlich darlegt. Die in der Resolution des Ministerrates benannte „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung“ ist ein Widerspruch in sich selbst. Verschlüsselung funktioniert entweder ausnahmslos, oder sie funktioniert gar nicht. Eine funktionierende Verschlüsselung, die nur für die Sicherheitsbehörden eine Ausnahme schafft, ist nicht denkbar und nicht möglich, wie zahlreiche Kryptographie-Expertinnen und –Experten wiederholt dargelegt haben. Jedes technische Mittel des Zugriffs auf verschlüsselte Kommunikation würde die Vertraulichkeit der Daten aller Nutzerinnen und Nutzer schwächen und die Bürger und Dienste einem erhöhten Risiko von Angriffen durch Hacker und ausländische Geheimdienste aussetzen, selbst wenn die vorgeschlagene Lösung „den Prinzipien der Legalität, Transparenz, Notwendigkeit und Verhältnismäßigkeit“ entsprechen würde.

Über die Risiken für die breite Masse deutscher Bürgerinnen und Bürger hinaus würde insbesondere die Vertraulichkeit der Kommunikation von Journalistinnen und Journalisten massiv gefährdet, ebenso wie der Schutz der Identität ihrer Quellen. Ende-zu-Ende-verschlüsselte Messengerdienste sind für Medienschaffende im digitalen Zeitalter ein wesentliches Recherche-und Kommunikationsmittel, dessen Schwächung zu nicht hinzunehmenden Kollateralschäden führen würde.

Aus eben diesen Gründen ist auch das in Abschnitt 8.3.8 angesprochene Schwachstellenmanagement kritisch zu sehen, mithilfe dessen **das gezielte Ausnutzen von Sicherheitslücken durch Nachrichtendienste und Strafverfolgungsbehörden** geregelt werden soll. Zahlreiche Sicherheitsexpertinnen und -experten haben wiederholt auf die Risiken einer solchen Strategie für die IT-Sicherheit hingewiesen. Untermauert werden diese Bedenken durch reale Vorfälle, bei denen erst das bewusste staatliche Offenhalten von Sicherheitslücken Dritten ermöglicht hat, illegal in fremde Systeme einzugreifen – mit teils gravierenden Folgen für die Öffentlichkeit (man denke beispielsweise an den WannaCry-Angriff). Vor diesem Hintergrund raten wir dringend zu einer strategischen Fokussierung auf die bestmögliche Absicherung der Integrität technischer Systeme. Das angesprochene übergeordnete **Ziel des „Security by design“ ist mit immer weitreichenderen staatlichen Zugriffsmöglichkeiten und bewusst offen gehaltenen Sicherheitslücken nicht vereinbar**.

Gleiches gilt für die anvisierte erweiterte Anwendung von Quellen-TKÜ und Online-Durchsuchung zur Strafverfolgung im Bereich der Cyberkriminalität. Statt über einen immer breiteren Anwendungsbereich zu sprechen, sollten zunächst die Notwendigkeit, Wirksamkeit und die Verhältnismäßigkeit dieser Überwachungsmaßnahmen in den bestehenden Anwendungsbereichen überprüft werden. Der vorliegende Vorschlag wiegt umso schwerer, da er den Einsatz der erwähnten Überwachungsbefugnisse in Bezug auf Verstöße gegen den Datenhehlerei-Paragraphen einschließt, der durch seine unpräzise Formulierung einen wichtigen Teil der Arbeit investigativer Journalistinnen und Blogger sowie ihrer Quellen und Fachberater kriminalisiert. Der Paragraph ist Gegenstand einer anhängigen Verfassungsbeschwerde von Reporter ohne Grenzen und weiteren Akteuren. **RSF**

empfiehlt daher dringend, der mehrmals in dem Kapitel angesprochenen Prüfung möglicher neuer Ermittlungskompetenzen der Sicherheitsbehörden **eine Überprüfung bestehender Strafrechtsnormen, Ermittlungsbefugnisse und der Verhältnismäßigkeit der daraus resultierenden Grundrechtseingriffe voranzustellen.**