Berlin, 17.07.2023

Stellungnahme und Kommentierung des Bundesverbandes IT-Sicherheit e.V. (TeleTrusT) zur Nichtannahme der Verfassungsbeschwerde gegen das "Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens" ein, insoweit der Gesetzgeber darin die Rechtsgrundlagen für die Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) und die Online-Durchsuchung erweitert und Grundrechte in Bezug auf das Fernmeldegeheimnis einschränkt, bzw. gegen den mit dem Gesetz legalisierten Einsatz von sog. "Staatstrojanern"

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Fachleute, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Personenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie des Vertrauenszeichens "IT Security made in Germany". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Chausseestraße 17
10115 Berlin
Tel.: +49 30 4005 4310
https://www. TeleTrusT.de

Gemäß Beschluss der Mitgliederversammlung 2017 legte der Bundesverband IT-Sicherheit e.V. (TeleTrusT), hier vertreten durch Prof. Dr. Norbert Pohlmann, RA Karsten U. Bartels LL.M. und Dr. Holger Mühlbauer als formelle Beschwerdeführer, am 19.04.2018 Verfassungsbeschwerde gegen das vom Deutschen Bundestag beschlossene und in Kraft getretene "Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens" ein, insoweit der Gesetzgeber darin die Rechtsgrundlagen für die Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) und die Online-Durchsuchung erweitert und Grundrechte in Bezug auf das Fernmeldegeheimnis einschränkt, bzw. gegen den mit dem Gesetz legalisierten Einsatz von sog. "Staatstrojanern".

Nach mehrjähriger Bearbeitungsdauer nahm das Bundesverfassungsgericht per Beschluss vom 17.04.2023 die Verfassungsbeschwerde nicht zur Entscheidung an (AZ 176/23 bzw. 178/23).

Der Bundesverband IT-Sicherheit kommentiert und kritisiert die Nichtannahme wie folgt:

Problem erkannt, Lösung verweigert

I. Hintergrund

Im August 2017 hat der Gesetzgeber die hoch umstrittene Online-Durchsuchung und Quellen-Kommunikationsüberwachung erstmals auch zu strafprozessualen Zwecken erlaubt. Die Vorschriften gestatten die heimliche Infiltration von informationstechnischen Systemen wie Mobiltelefonen, Tablets und Computern zum Aufspielen von Überwachungssoftware (den sogenannten "Staatstrojanern“). Damit soll es Ermittlern ermöglicht werden, Kommunikation und Daten an den Endgeräten auszulesen, bevor sie verschlüsselt werden. Um eine solche Infiltration zu ermöglichen und die Software unbemerkt zu platzieren, muss zunächst ein Zugang zum Zielsystem eröffnet werden. Hierzu sind die Ermittler in der Regel (nicht anders als die Anwender herkömmlicher Schadsoftware) auf bestehende Sicherheitslücken in den IT-Systemen angewiesen, die sie entdecken oder ankaufen und ausnutzen müssen, bevor sie geschlossen werden. Mit der Einführung solcher Maßnahmen, die sich neben der Strafprozessordnung auch in einer Vielzahl von Polizei- und Nachrichtendienstgesetzen finden, wurde ein grundsätzlicher Zielkonflikt eingeläutet zwischen dem staatlichen Interesse an der Offenhaltung dieser gefährlichen Sicherheitslücken und dem Interesse der Allgemeinheit an größtmöglicher IT-Sicherheit, zu deren Gewährleistung sich Regierung und staatliche Stellen vielfach verpflichtet haben.

II. Die Verfassungsbeschwerde des Bundesverbandes IT-Sicherheit e. V. (TeleTrusT)

Die im Jahr 2018 erhobene Verfassungsbeschwerde des Bundesverbandes IT-Sicherheit e.V. (TeleTrusT) hat deshalb neben anderen Punkten insbesondere gerügt, dass die Einführung solcher Befugnisse mit einer unvertretbaren Schwächung der allgemeinen IT-Sicherheit einhergeht. Die Argumentation stützte sich vor allem auf das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ("IT-Grundrecht“), das das Bundesverfassungsgericht in seiner Entscheidung vom 27.02.2008 (BVerfGE 120, 274 - Verfassungswidrigkeit der Online-Durchsuchung im Verfassungsschutzgesetz NRW) in einer seiner ersten Auseinandersetzungen mit dem Thema Online-Durchsuchung entwickelt hatte. Die Verfassungsbeschwerde von TeleTrusT hat diesbezüglich zwei Kernaussagen getroffen:

Erstens erschöpft sich dieses Grundrecht nicht darin, einzelnen Betroffenen ein Abwehrschild gegenüber unverhältnismäßigen Eingriffen in ihre digitale Privatsphäre zu bieten, sondern beinhaltet darüber hinaus eine **aktive Schutzpflicht** des Staates, die IT-Sicherheit der Bevölkerung zu gewährleisten und sich schützend vor sie zu stellen. Diese Frage war damals Gegenstand juristischer Debatten und durch die Rechtsprechung noch nicht beantwortet.

Und zweitens: der Gesetzgeber verstößt gegen diese Schutzpflicht, wenn er seine Behörden mit Überwachungsbefugnissen ausstattet, die es erforderlich machen, Schutzlücken auszunutzen, offenzuhalten und möglicherweise sogar auf dem schwarzen oder grauen Markt anzukaufen, anstatt sie möglichst schnell den Herstellern bekannt zu machen, damit diese die Lücken schließen. So werden Bestrebungen für die IT-Sicherheit konterkariert. Denn eine Sicherheitslücke kann, solange sie offen ist, nicht nur von den staatlichen Stellen, sondern von jedermann zu beliebigen Zwecken genutzt werden. Unter Ausnutzung solcher Vulnerabilitäten werden bekanntlich Jahr für Jahr Milliardenschäden angerichtet, Daten gestohlen und Kritische Infrastrukturen gefährdet. Staatliche Behörden dürfen solche Gefahren schon nicht setzen. Im Gegenteil muss der Staat diesen einen Mindestumfang gesetzlicher Regulierung gegenüberstellen, der die IT-Sicherheit hinreichend schützt. Dabei geht es konkret um ein geeignetes **"Schwachstellen-Management“**, also um klare gesetzliche Regeln, wie Ermittlungsbehörden mit Sicherheitslücken umgehen sollen - also die Feststellung, dass nicht nach Belieben

Lücken ausgenutzt, offengehalten oder gar angekauft werden dürfen, und die Festlegung, welche Faktoren in die Abwägung darüber einzufließen haben (beispielsweise Ausmaß und Gewicht der Lücke, Nutzen für Ermittlungszwecke und ähnliches). Solche hinreichenden gesetzlichen Regelungen gab es weder bei Erhebung der Verfassungsbeschwerde noch gibt es sie heute.

III. Teilerfolge zu IT-Sicherheitslücken und Schwachstellen-Management seit 2018

Seit Erhebung der Verfassungsbeschwerde im Jahr 2018 sind mehr als fünf Jahre vergangen. Das ist für Entscheidungen des Bundesverfassungsgerichts über Verfassungsbeschwerden, die Gesetze angreifen, nicht ganz außergewöhnlich, aber hat doch dazu geführt, dass sich sowohl die politische als auch juristische Debatte weiterentwickelt haben.

Am 08.06.2021 hat das Bundesverfassungsgericht eine Beschwerde gegen das Polizeigesetz Baden-Württemberg zurückgewiesen (BVerfGE 158, 170 - IT-Sicherheitslücken), aber zugleich die auch von der Verfassungsbeschwerde von TeleTrusT ins Feld geführte aktive Schutzpflicht zum Schutz informationstechnischer Systeme anerkannt:

> *"Die grundrechtliche Schutzpflicht des Staates verlangt auch eine Regelung zur grundrechtskonformen Auflösung des Zielkonflikts zwischen dem Schutz informationstechnischer Systeme vor Angriffen Dritter mittels unbekannter Sicherheitslücken einerseits und der Offenhaltung solcher Lücken zur Ermöglichung einer der Gefahrenabwehr dienenden Quellen-Telekommunikationsüberwachung andererseits."* (BVerfGE 158, 170 [Tenor zu 2. b)])

Das Anerkennen dieser Schutzpflicht wurde aus datenschutzrechtlicher Sicht als wesentlicher Erfolg angesehen. Damit war ein Kernpunkt bereits im Sinne der Verfassungsbeschwerde von TeleTrusT entschieden. Zugleich war die Entscheidung problematisch, da das Bundesverfassungsgericht einerseits sogar die Ausnutzung von Zero-Day-Lücken für grundsätzlich gangbar gehalten hatte und andererseits bewusst davon abgesehen hatte, die Frage, ob der Staat ohne Schwachstellen-Management dieser Schutzpflicht derzeit gerecht wird oder nicht, zu beantworten. Es bestünden *"unterschiedliche gesetzliche Regelungen zum Schutz informationstechnischer Systeme, denen - ohne dass dies hier abschließend verfassungsrechtlich bewertet werden kann - auch im vorliegenden Kontext Bedeutung zukommen könnte"* (BVerfGE 158, 170 [192]). So sei es beispielsweise zweifelhaft, aber doch denkbar, dass beim Offenhalten einer Zero-Day-Sicherheitslücke eine Datenschutz-Folgenabschätzung erstellt werden müsse, die zur Erfüllung der staatlichen Schutzpflicht beitragen könne. Es sei nicht Aufgabe des Bundesverfassungsgerichts, das Fachrecht eigenständig daraufhin auszuleuchten, inwiefern als Schutznormen in Betracht kommende Regelungen dem grundrechtlichen Schutzauftrag gerecht werden oder diesen aber verfehlen. Die Beschwerde sei deshalb in diesem Punkt unzulässig.

Dieser Rückzug aus der entscheidenden inhaltlichen Diskussion auf das Argument unzureichenden Beschwerdevortrags sollte sich in ähnlichen Entscheidungen fortsetzen, etwa in der Entscheidung über eine Verfassungsbeschwerde gegen das Gesetz über die öffentliche Sicherheit und Ordnung in Mecklenburg-Vorpommern vom 9. Dezember 2022 (1 BvR 1345/21), in der es ebenfalls heißt, die Beschwerdeführer hätten näher darauf eingehen müssen, dass möglicherweise auch beim Offenhalten einer Sicherheitslücke eine Datenschutz-Folgenabschätzung vorzunehmen sei (a.a.O., Rn. 67).

Dass der gegenwärtige, also nahezu nicht existente Regelungsrahmen nicht als offensichtlich ungenügend erkannt wird, ist schwer nachzuvollziehen. Denn dass die Ausnutzung von Schwachstellen durch Strafverfolgungs- und Sicherheitsbehörden derzeit nicht hinreichend geregelt ist und der Staat deshalb für seine damit befassten Behörden dringend ein Schwachstellen-Management etablieren und hierzu verbindliche Regeln einführen muss, ist in Politik und Wissenschaft heute weitgehend anerkannt. So stellt der aktuelle Koalitionsvertrag zwischen SPD, Bündnis 90/Die Grünen und FDP fest:

> *"Die Ausnutzung von Schwachstellen von IT-Systemen steht in einem hochproblematischen Spannungsverhältnis zur IT-Sicherheit und den Bürgerrechten. Der Staat wird daher keine Sicherheitslücken ankaufen oder offenhalten, sondern sich in einem Schwachstellenmanagement unter Federführung eines unabhängigeren Bundesamtes für Sicherheit in der Informationstechnik immer um die schnellstmögliche Schließung bemühen."* (Koalitionsvertrag 2021 - 2025, S. 109)

Das Bundesministerium des Innern und für Heimat hat auf seine Liste der "Zentralen Vorhaben des BMI 2022/2023" notiert, es stehe die "Einführung eines wirksamen Schwachstellenmanagements" an (Zentrale Vorhaben des BMI 2022/2023, S. 2). Und das Bundesamtes für Sicherheit in der Informationstechnik (BSI), das laut Koalitionsvertrag die Federführung für das noch einzuführende Schwachstellen-Management übernehmen

soll, sieht dies sogar noch in erheblicher Ferne, da noch nicht einmal die fundamentalen Rahmenbedingungen feststünden und das BSI dabei in einen ungelösten Konflikt mit den Sicherheitsbehörden gerate:

> *"Bevor überhaupt gesetzliche Regelungen zum staatlichen Umgang mit Schwachstellen geschaffen werden können, ist es hiesigen Erachtens notwendig, die Ziele, Definitionen und Rahmenbedingungen eines geplanten Schwachstellenmanagements festzulegen. So ist, rein auf Basis der Aussagen des Koalitionsvertrages, nicht klar, ob es sich bei dem Konzept um eine Art Coordinated Vulnerability Disclosure (CVD-Prozess), eine Art Vulnerabilities Equities Process (VEP), oder um beides inklusive darüberhinausgehender Maßnahmen handelt. […] Die Pflichten des Staates zum Schutz der unterschiedlichen Grundrechte führen im Kontext der IT-Sicherheit und öffentlichen Sicherheit, wie am staatlichen Umgang mit Zero-Days deutlich wird, in einen Zielkonflikt staatlicher Sicherheitspolitik und damit innerhalb der Cybersicherheitsarchitektur Deutschlands, qua unterschiedlicher gesetzlicher Aufträge, auch zu einem Interessenkonflikt zwischen dem BSI und den Sicherheitsbehörden."* (Antworten des Bundesamtes für Sicherheit in der Informationstechnik – BSI - auf den Fragenkatalog zur Öffentlichen Anhörung des Ausschusses für Digitales am 25.01.2023 "Cybersicherheit - Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland", Ausschuss-Drucksache 20(23)125, S. 11 f.)

In dieser Entwicklung zeigt sich zudem, dass sich die Forderung nach einem Schwachstellen-Management, die TeleTrusT in seiner Verfassungsbeschwerde bereits 2018 erhoben hat, inzwischen in aller gesellschaftlicher Breite etabliert hat - wenngleich dies noch nicht zu einer praktischen Umsetzung geführt hat. Dabei ist stets darauf hinzuweisen, dass ein irgendwie geartetes Schwachstellen-Management nicht dazu führt, dass die staatliche Ausnutzung von Sicherheitslücken ungefährlich würde. Umgekehrt weist der staatliche Umgang damit ohne Schwachstellen-Management aber jedenfalls nicht einmal die Minimalstandards auf.

IV. Entscheidung des Bundesverfassungsgerichts über die Verfassungsbeschwerde von TeleTrusT

Mit Beschluss vom 17.04.2023 hat das Bundesverfassungsgericht durch die 2. Kammer des Ersten Senats die 2018 von TeleTrusT erhobene Verfassungsbeschwerde nicht zur Entscheidung angenommen.[1] Angesichts der oben beschriebenen Entwicklungen kann dies nicht völlig überraschen, ist aber doch aus mehreren Gründen enttäuschend. Der Beschluss macht in seiner knappen Begründung Anmerkungen zu zwei Punkten, die bei der Ablehnung von Beschwerden gegen Überwachungsbefugnisse häufig zu finden sind:

Erstens könnten die Beschwerdeführer nicht geltend machen, durch die Gesetze selbst in ihren Grundrechten betroffen zu sein. Dies betrifft eine grundsätzliche Problematik zum Rechtsschutz gegen Überwachungsbefugnisse. Die Bürger sind zunächst gehalten, sich gegen den konkreten Eingriff zu wehren, also hier beispielsweise eine sie betreffende Online-Durchsuchung. Da die Maßnahme aber heimlich stattfindet, wissen die Betroffenen zunächst nichts von ihrer tatsächlichen Betroffenheit. Dafür muss aber gezeigt werden, dass man zukünftig mit einiger Wahrscheinlichkeit von einer solchen Maßnahme betroffen sein wird. Hier muss der Beschwerdeführer argumentieren, warum er glaubt, in den Zielbereich der Maßnahme geraten zu können, obwohl diese Entscheidung einzig bei den dazu befugten Behörden (und in der Zukunft) liegt. Das macht es grundsätzlich schwierig, solche Überwachungsbefugnisse erfolgreich anzugreifen. Vorliegend spricht bereits die hohe Streubreite der Maßnahme, die immerhin auch all diejenigen betreffen kann, die mit einer überwachten Person kommunizieren und sich sogar gegen Dritte richten darf, deren Systeme durch einen Beschuldigten genutzt werden, für die Wahrscheinlichkeit einer Betroffenheit spricht. Zudem haben die Beschwerdeführer dargelegt, dass sie aufgrund ihrer professionellen Tätigkeit mit Verschlüsselungstechnologien, IT-Sicherheit und Datenschutz im Hochrisikobereich beruflich mit Personen in Kontakt kommen, gegen welche die hier gegenständlichen Maßnahmen eingesetzt werden können (wie etwa bei den Themenkreisen Schutz von Whistleblowern, Entwicklung von Sicherheitslösungen im Angesicht des Zugriffs internationaler Nachrichtendienste oder Cyber-War und -Spionage oder bei der Tätigkeit als Rechtsanwalt, der berufsbedingt regelmäßig in Kontakt mit möglicherweise strafrechtlich relevanten Sachverhalten im Sinne der Eingriffsbefugnis kommt).

Hinzu tritt, dass die mit den Überwachungsbefugnissen einhergehende Verletzung der IT-Schutzpflicht gerade nicht nur die von einer konkreten Maßnahme betroffenen berührt, sondern die gesamte IT-Sicherheit. Insbesondere die geschaffenen Anreize zum Offenhalten von Sicherheitslücken schwächt die Sicherheitsmechanismen, die die Beschwerdeführer betreuen, entwickeln und einsetzen, und das darin gesetzte Vertrauen. Gleichwohl hat das Bundesverfassungsgericht keine Selbstbetroffenheit der Beschwerdeführer erkennen wollen, ohne dies

[1] Die "Nichtannahme" ist das mit Abstand häufigste Entscheidungsformat und schließt nicht aus, dass das Gericht zugleich inhaltliche Ausführungen macht. Zur Einordnung aus der Jahresstatistik 2021: Von 5.059 eingegangenen Verfassungsbeschwerden wurden 97,7 % nicht zur Entscheidung angenommen.

weiter zu begründen oder auf den Vortrag einzugehen. Auch diese Argumentation ist für solche Beschwerdeverfahren typisch. So verweist der vorliegende Beschluss etwa auf die bereits zitierte Entscheidung zur Online-Durchsuchung im Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommern, in der ebenfalls mehrere Beschwerdeführer mit dieser Begründung auf formeller Ebene abgewiesen wurden (1 BvR 1345/21, Rn. 54 ff.). Diese Art der Abarbeitung ist einerseits deshalb bedenklich, weil dies den Rechtsschutz der Bürger gegen heimliche Überwachungsbefugnisse sehr eng auslegt. Zudem wird die (ohnehin unausweichliche) verfassungsrechtliche Auseinandersetzung mit der strafprozessualen Online-Durchsuchung und Quellen-Telekommunikationsüberwachung aus formellen, nicht näher ausgeführten Gründen abgeschnitten, obwohl es auf der Hand liegt, dass die Verfassungsbeschwerde inhaltlich gewichtige Argumente vorbringt, die auch von anderen Verfassungsbeschwerden, von Politik und Rechtswissenschaft und wie gezeigt sogar durch das Bundesverfassungsgericht selbst geteilt werden.

Zweitens verweist der Beschluss auf die genannten Entscheidungen aus den letzten beiden Jahren, wonach zwar eine aktive Schutzpflicht bestehe, die Aufarbeitung, inwieweit der bisherige gesetzliche Rahmen dem genügt, aber nicht Sache des Gerichts sei - ebenfalls unter Verweis auf die Frage, ob der staatlichen Schutzpflicht möglicherweise im Rahmen einer Datenschutz-Folgenabschätzung genüge getan werden könnte. Dieser Verweis zeugt, wie auch schon in den vorangegangenen Entscheidungen, von einer unsachgemäßen Vermengung von Rechtspflichten und deren Anwendungsbereichen. Eine Datenschutz-Folgenabschätzung stellt keinen hinreichenden Schutzmechanismus im Sinne von IT-Schutzpflicht gegenüber der Ausnutzung von Sicherheitslükken dar. Eine Datenschutz-Folgenabschätzung ist eine Risikobewertung zur Sicherstellung allein datenschutzrechtlicher Pflichten. Die grundsätzlichen Risiken, die insbesondere mit der Offenhaltung von Zero-Day-Schwachstellen einhergeht, werden nicht gewürdigt. Nicht zuletzt angesichts des Umstandes, dass heute von breiten Teilen von Wissenschaft, Politik und Bevölkerung konkrete, transparente und vor allem gesetzlich verbindliche Regelungen zum Umgang der Ermittlungs- und Sicherheitsbehörden mit IT-Sicherheitslücken für unerlässlich gehalten werden, senden Entscheidungen wie diese ein falsches Signal.

Zwar ist die jetzige Entscheidung teilweise auch eine Konsequenz der Entwicklungen seit 2018 bzw. des diskursiven und juristischen Erfolgs der vorgetragenen Argumentation. Zugleich bleibt festzuhalten: Die Auseinandersetzung mit dem offensichtlich ungenügenden staatlichen Schwachstellen-Management und dem Umstand, dass Befugnisse zur Nutzung von "Staatstrojanern“ eingeführt wurden, ohne die damit geschaffenen Gefahren für die allgemeine IT-Sicherheit mitzudenken, darf nicht länger aufgeschoben werden.