PRESSEMITTEILUNG

Problem erkannt, Lösung verweigert: Stellungnahme und Kritik des Bundesverbandes IT-Sicherheit e.V. (TeleTrusT) zur Nichtannahme der Verfassungsbeschwerde gegen den legalisierten Einsatz von "Staatstrojanern"

Berlin, 17.07.2023 - Im Jahr 2018 legte der Bundesverband IT-Sicherheit e.V. (TeleTrusT) Verfassungsbeschwerde gegen den per Gesetz legalisierten Einsatz von "Staatstrojanern" ein. Das Bundesverfassungsgericht nahm per Beschluss vom 17.04.2023 die Verfassungsbeschwerde nicht zur Entscheidung an. TeleTrusT kritisiert die Nichtannahme in einer Stellungnahme.

Gemäß Beschluss der TeleTrusT-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.

Mit der Einführung der mit der Verfassungsbeschwerde beanstandeten 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.

Die von TeleTrusT 2018 erhobene Verfassungsbeschwerde 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.

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.

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. 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.

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 Sicherheitslücken dar.

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.

RA Karsten U. Bartels LL.M., HK2 RAe und stellvertretender TeleTrusT-Vorsitzender, kommentiert: "Die Verfassungsbeschwerde nicht zur Entscheidung anzunehmen, ist mehrfach enttäuschend. Das Bundesverfassungsgericht befasst sich nicht nur zu verkürzt mit der Betroffenheit der Beschwerdeführer. Es umgeht so auch die überfällige Befassung mit der Frage, wie der Staat die IT-Sicherheit konkret zu schützen - jedenfalls nicht zu unterminieren hat. Die Auswirkungen der Staatstrojaner scheinen nicht realisiert und die rechtliche Rolle des Datenschutzes verkannt zu werden. Es ist unvertretbar, für diesen Beschluss fünf Jahre ins Land gehen zu lassen."

Ausführlicher Text der TeleTrusT-Stellungnahme: https://www.teletrust.de/publikationen/stellungnahmen/

Bundesverband IT-Sicherheit e.V. (TeleTrusT), Dr. Holger Mühlbauer, Geschäftsführer, Chausseestraße 17, 10115 Berlin, Tel.: +49 30 40054310, holger.muehlbauer@teletrust.de
https://www.teletrust.de