neues deutschland SOZIALISTISCHE TAGESZEITUNG 22.08.2018
https://www.neues-deutschland.de/artikel/1098014.ueberwachung-hinterlist-im-staatsauftrag.html

Hinterlist im Staatsauftrag

Der Staatstrojaner ist ein Einbruch in Grund- und Freiheitsrechte

Von **Rolf Gössner** / 22.08.2018

Staatstrojaner sind digitale Waffen, mit denen der Staat heimlich in Privatsphäre und Persönlichkeitsrechte, in Informationelle Selbstbestimmung und Meinungsfreiheit der Betroffenen einbrechen kann. Es handelt sich um einen der schwersten Grundrechtseingriffe, der auch die Menschenwürde verletzt sowie die IT-Sicherheit schädigt - und damit die Allgemeinheit. Diese Methode zur digitalen Totalüberwachung gehört deshalb dringend für null und nichtig erklärt.

Unsere Verfassungsbeschwerde richtet sich gegen Normen der Strafprozessordnung, die die Strafverfolgungsorgane dazu ermächtigen, mit technischen Mitteln heimlich »informationstechnische Systeme« anzugreifen. Das heißt: Die Polizei als Ermittlungsorgan der Staatsanwaltschaft darf im Rahmen der Strafverfolgung zur verdeckten Informationsgewinnung Computersysteme, PC, Tablets, Smartphones mit Hilfe von Spionageprogrammen hacken - mit Hilfe der berüchtigten »Staatstrojaner«. Diese Überwachungssoftware wird unter Ausnutzung von Sicherheitslücken heimlich in digitale Endgeräte von Verdächtigten eingeschleust, um diese ausforschen zu können - mittels Quellen-Telekommunikationsüberwachung oder Online-Durchsuchung.

Die richterliche Anordnung solcher Maßnahmen ist auf ein oder drei Monate zu befristen, kann aber verlängert werden und das letztlich ohne zeitliche Begrenzung - unseres Erachtens ein Verstoß gegen den Verfassungsgrundsatz der Verhältnismäßigkeit. Mit diesen Methoden, die der Verfolgung besonders schwerer Straftaten dienen sollen, bricht der Staat massiv in Privatsphäre und Persönlichkeitsrechte, in Informationelle Selbstbestimmung und Meinungsfreiheit der Betroffenen ein – aber auch von bloßen Kontaktpersonen, denn solche Maßnahmen dürfen unter bestimmten Voraussetzungen auch gegen sie durchgeführt werden und auf alle Fälle auch, wenn unbeteiligte Dritte „unvermeidbar" betroffen werden.

Mit Hilfe der Trojaner kann die Polizei unbemerkt sämtliche laufenden Kommunikationsinhalte vor ihrer Verschlüsselung überwachen - inklusive SMS, Mails, Chats und Messenger-Dienste. Oder aber im Fall der Online-Durchsuchung auf sämtliche Datenbewegungen, auf alle gespeicherten Festplatten-Inhalte, auf Textdokumente, Gesundheits- und Finanzdaten, auf intimste Informationen, Fotos und Filme zugreifen - letztlich auf das gesamte digitale und vernetzte Leben der Betroffenen. Angesichts dieser digitalen Totalüberwachung und der hieraus entstehenden Persönlichkeits-, Kontakt- und Bewegungsprofile ist an den verfassungsrechtlich gebotenen Schutz des *Kernbereichs persönlicher Lebensgestaltung* praktisch nicht mehr zu denken – ganz abgesehen davon, dass solche Geheimmethoden weder gerichtlich noch parlamentarisch wirklich wirksam kontrollierbar sind.

Es handelt sich um einen der schwersten staatlichen Grundrechtseingriffe – um einen Einbruch in alle Lebensbereiche. Wobei mit diesen Maßnahmen auch PC-Mikrofone und Webcams eingeschaltet und auf diese Weise Wohnungen oder Büros ausgespäht werden können. Heribert Prantl von der „Süddeutschen Zeitung" spricht insoweit zu Recht von „digitaler Inquisition", vor der nichts und niemand sicher sei.

Staatstrojaner sind digitale Waffen, die nicht nur Bürger- und Freiheitsrechte der Betroffenen unterminieren, sondern auch deren Menschenwürde – und darüber hinaus auch noch das *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*, wie es das Bundesverfassungsgericht für das digitale Zeitalter als „Computergrundrecht" aus der Taufe gehoben hat. Denn

die Polizei muss Software-Sicherheitslücken ausfindig machen, um einen Staatstrojaner auf dem Gerät installieren zu können. Sie wird versuchen, solche Schwachstellen für eigene Zwecke auch künftig offenzuhalten – anstatt sie sofort schließen zu lassen, um Attacken Dritter abzuwehren und so das IT-System insgesamt zu schützen und damit die Allgemeinheit. Stattdessen werden mutwillig Sicherheitslecks als Einfallstore aufrechterhalten, über die auch Geheimdienste, Cyber-Kriminelle, Betrüger, Erpresser und Terroristen gefährliche Angriffe auf private, betriebliche oder staatliche Computersysteme ausführen können oder auf kritische Infrastrukturen - etwa von Strom- und Wasserversorgern, des Krankenhaus-, Gesundheits- oder Verkehrswesens.

Dieses unverantwortliche Staatsverhalten öffnet Missbrauch und gefährlichen Cyberattacken Tür und Tor. Abschreckendes Beispiel: der Erpressungstrojaner „Wannacry", der 2017 neben Privat-PCs auch Automobilkonzerne, Bahnunternehmen und Krankenhäuser lahmlegte und Schäden in Millionenhöhe verursachte. Die dabei genutzte Sicherheitslücke war dem US-Geheimdienst NSA bereits seit Jahren bekannt. Verantwortungsvolle Sicherheitspolitik, die diese Bezeichnung verdient, sieht anders aus. Denn es gehört zum Auftrag des Staates, seine Bürger zu schützen und Sicherheitslücken zu schließen, und nicht, sie mutwillig für eigene Trojaner sperrangelweit offenzuhalten – und damit eben auch für andere Cyberangreifer.

Inzwischen haben die Justizminister_innen des Bundes und der Länder auf ihrer Frühjahrskonferenz 2018 die Bundesjustizministerin ersucht, die *„Schaffung eines gesetzlichen Betretungsrechts zum Zwecke der Aufbringung der Software als zielführende Alternative*" zur derzeit zulässigen Möglichkeit der Einschleusung in informationstechnische Systeme zu prüfen und zu legalisieren. Das heißt: Die Polizei soll sich heimlich oder aber per Trick - etwa über Handwerker - Zutritt in Wohnungen verschaffen dürfen, um Schadsoftware direkt vor Ort auf Computer oder Smartphones aufzuspielen – das wäre dann ein doppelter Einbruch.

Insgesamt gesehen handelt es sich bei diesen Regelungen in Strafprozessordnung und etlichen Polizeigesetzen um einen weiteren Schritt in Richtung eines präventiven Sicherheitsstaates, der seit 9/11 im Zuge einer ausufernden Sicherheits- und Antiterrorpolitik längst schon bedrohliche Konturen angenommen hat und derzeit mit der Verschärfung der Polizeigesetze noch weiter ausgebaut wird.

Wie nötig gerade auch in diesem Fall eine Verfassungsbeschwerde ist, zeigt die hohe Anzahl von Sicherheits- und Antiterror-Gesetzen, die in den letzten Jahren und Jahrzehnten ganz oder teilweise für verfassungswidrig erklärt werden mussten. Die Verfassungsgerichte rügen in all diesen Fällen, dass Regierungen und Parlamentsmehrheiten Grund- und Bürgerrechte, die Menschenwürde und den Kern privater Lebensgestaltung unhaltbaren Sicherheitsversprechen und einer vermeintlichen Sicherheit geopfert haben. Diese hohe Anzahl verfassungswidriger Gesetze dokumentiert ein bedenkliches Verfassungsbewusstsein in der politischen Klasse – strenggenommen: ein Fall für den „Verfassungsschutz".

Foto: dpa/Karl-Josef Hildenbrand

Dr. Rolf Gössner, einer der Beschwerdeführer gegen den Staatstrojaner, ist Rechtsanwalt, Publizist und Kuratoriumsmitglied der *Internationalen Liga für Menschenrechte* (Berlin). Mitherausgeber des jährlich erscheinenden *"Grundrechte-Reports. Zur Lage der Bürger- und Menschenrechte in Deutschland"* sowie Mitglied der Jury zur Verleihung des Negativpreises *BigBrotherAward.* Ausgezeichnet mit der Theodor-Heuss-Medaille, dem Kölner Karlspreis für engagierte Literatur und Publizistik und dem Bremer Kultur- und Friedenspreis. Sachverständiger in Gesetzgebungsverfahren von Bundestag und Landtagen. Autor zahlreicher Bücher zum Themenbereich Demokratie, Innere Sicherheit und Bürgerrechte.