Gute Lücken, schlechte Lücken? Zur objektiv-rechtlichen Dimension des IT-Grundrechts

Ulf Buermeyer 2018-09-08T18:00:59

Staatliches Hacking von Computern und Smartphones hat Konjunktur. Durch das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017 (BGBl. I S. 3202) wurden Online-Durchsuchung und Quellen-TKÜ mittels „Staatstrojanern“ zu Standardmaßnahmen im strafrechtlichen Ermittlungsverfahren. Die StPO erlaubt seither den Einsatz von Staatstrojanern in mehreren zehntausend Fällen im Jahr: Sie sind nun immer dann zulässig, wenn bisher eine klassische Telekommunikationsüberwachung gem. § 100a Abs. 1 StPO unter Einbindung der jeweiligen Provider (vgl. § 100b StPO a.F.) vorgenommen wurde.

Verfassungsbeschwerde gegen den „Staatstrojaner“

Gegen diese extreme Ausweitung des staatlichen Hackings wenden sich mehrere Beschwerdeführer und eine Beschwerdeführerin (im Folgenden: die Bf.) mit einer Verfassungsbeschwerde, die die Gesellschaft für Freiheitsrechte e.V. koordiniert hat. Die Verfassungsbeschwerde rügt zunächst einige Details der Rechtsgrundlagen in der StPO, die mit den Maßstäben von BVerfGE 120, 274 („Online-Durchsuchung“) für den Einsatz von Staatstrojanern nicht im Einklang stehen. Die Bf. setzen sich dafür ein, dass das BVerfG die Schranken des „Grundrechts auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme“ (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, im Folgenden: IT-Grundrecht), welche das Gericht für den präventiven Bereich entwickelt hat, auf die Strafverfolgung überträgt.

Daneben rügen die Bf. vor allem eine Leerstelle: Der Bund ist bisher seinen Verpflichtungen nicht nachgekommen, die sich aus der objektiv-rechtlichen Dimension des IT-Grundrechts ergeben. Insbesondere hat der Gesetzgeber es vollständig versäumt, einen Rechtsrahmen für den Einsatz von Staatstrojanern zu schaffen, der geeignet ist, fatale Fehlanreize für Behörden des Bundes und der Länder zu vermeiden. Der Gesetzgeber lässt den Behörden bisher vollständig freie Hand, wie sie mit IT-Sicherheitslücken umgehen. Zwar billigt das BVerfG dem Gesetzgeber bei der Wahrnehmung von Schutzpflichten traditionell sehr weite Einschätzungsspielräume zu, ein vollständiges Ignorieren der aus dem IT-

Grundrecht resultierenden Schutzpflicht aber steht nicht mehr im Einklang mit den Anforderungen des Grundgesetzes.

Objektiv-rechtliche Dimension des IT-Grundrechts

Aber gibt das IT-Grundrecht tatsächlich eine Schutzpflicht her? Die Bf. und die GFF haben daran keinen Zweifel. Zum einen sei auf die gewählte Bezeichnung des Grundrechts („*Gewährleistung* der Integrität und Vertraulichkeit …“) verwiesen, die schon rein sprachlich ein aktives Tätigwerden verlangt, zum anderen auf die lange Tradition des BVerfG, in den Grundrechten nicht nur Abwehrrechte gegen staatliche Eingriffe, sondern objektiv-rechtliche Wertentscheidungen der Verfassung zu erkennen. Konsequenterweise hat das BVerfG bereits viele Grundrechte zu Schutzpflichten verdichtet – unter anderem das Grundrecht auf körperliche Unversehrtheit, das Post- und Fernmeldegeheimnis und das allgemeine Persönlichkeitsrecht.

Die Pflicht zum Schutz von IT-Systemen folgt aber auch aus der enormen Bedeutung, die IT-Systeme in der heutigen Gesellschaft haben: Computer und Smartphones werden nahezu flächendeckend in jedem Lebensbereich eingesetzt. Sie sind oft miteinander vernetzt, was ihre Verletzlichkeit potenziert. Und sie sind zentral geworden für die Wahrnehmung und Ausübung anderer Grundrechte wie der Wissenschafts-, Meinungs-, Presse-, Versammlungs-, Vereinigungs- und Berufsfreiheit. So wie der Staat physische Infrastrukturen zu sichern hat, so wie er selbstverständlich den Umgang mit Waffen durch Polizei und Militär oder mit Kernbrennstoffen durch die Betreiber von Atomkraftwerken strengen Regeln unterwirft, so muss er auch für die virtuelle Infrastruktur tatsächlich wirksame Schutzvorkehrungen treffen, indem er dafür sorgt, dass Sicherheitslücken in IT-Systemen so schnell wie möglich geschlossen werden. Zudem muss er für den eigenen Umgang mit virtuellen Waffen – denn nichts anderes sind Trojaner zur Ausnutzung von Sicherheitslücken in IT-Systemen –, Regelungen treffen, die tatsächlich geeignet sind, die Verletzlichkeit von IT-Systemen zu minimieren.

Die Erkenntnis, dass ehedem physisch beobachtbare Ereignisse nunmehr im Cyberspace stattfinden, ist ja richtig. Sie kann aber nicht lediglich dazu führen, dass staatliche Befugnisse in den virtuellen Raum erweitert werden, sondern geht Hand in Hand mit staatlichen Pflichten. Es zeichnet den Rechtsstaat aus, dass er neuen, ihm als ungezügelt, gar „rechtsfrei“ erscheinenden Räume nicht mit ebenso ungezügelten (trojanischen) Pferden, sondern umsichtig und verhältnismäßig begegnet. Dazu gehört auch ein verantwortungsvoller Umgang mit Schwachstellen in IT-Systemen, die den Herstellern noch nicht bekannt sind. Diese Umsicht lässt die gegenwärtige Rechtslage auf Bundesebene indes vermissen. Denn der Bund erlaubt es Ermittlungsbehörden mit §§ 100a Abs. 1 Satz 2, 100b StPO, in informationstechnische Systeme einzugreifen, um aus ihnen Daten zu erheben. Hierzu ist denklogisch ein „Fuß in der Tür“ erforderlich, also das Aufbringen einer

hoheitlichen Software, die Daten ausliest und an die Strafverfolgungsbehörden übermittelt – eben ein „Staatstrojaner“.

Weder die StPO in der angegriffenen Fassung noch die Begründung des entsprechenden Gesetzesentwurfs definieren indes, wie ein Staatstrojaner auf das Zielsystem aufgebracht werden darf. Denkbar ist hier zweierlei: zum einen das Ausnutzen der Unaufmerksamkeit des berechtigten Nutzers, etwa indem man ihm einen E-Mail-Anhang mit einem (getarnten) Infektions-Programm zuspielt, zum anderen das Ausnutzen von Sicherheitslücken derart, dass der berechtigte Nutzer zum Aufruf einer speziell präparierten Internetseite animiert wird, deren bloße Ansicht zur Infektion des Zielsystems führt (sogenannte drive by downloads). Beides ist vom Wortlaut der §§ 100a Abs. 1 Satz 2, 100b StPO gedeckt.

Letzteres führt aber zu gravierenden Fehlanreizen: Wenn Behörden bestehende Sicherheitslücken ausnutzen dürfen, haben sie ein Interesse daran, ein „Arsenal“ ebensolcher Sicherheitslücken aufzubauen, um im Falle des Falles eine Zielperson angreifen zu können. So entstehen Anreize für Behörden, ihnen bekannte Sicherheitslücken gerade nicht schließen zu lassen, sondern sie lieber zu „horten“. Schon heute kaufen staatliche Stellen Sicherheitslücken auf dem Schwarzmarkt auf bzw. haben entsprechende Mittel im Zuge der Haushaltsberatungen bewilligt bekommen. Dies führt nicht nur dazu, dass Sicherheitslücken nicht geschlossen werden. Vielmehr wird der bestehende Schwarzmarkt zusätzlich angeheizt. Steigende Preise für Sicherheitslücken wiederum schaffen Anreize für Sicherheitsforscher, ihre Erkenntnisse nicht den Herstellern zur Verfügung zu stellen, sondern sie zu verkaufen. Auf diese Weise bestehen Sicherheitslücken fort, die eigentlich schon geschlossen werden könnten. Diese kann jeder, der sie findet oder seinerseits auf dem Schwarzmarkt für Sicherheitslücken kauft, zur Infiltration informationstechnischer Systeme missbrauchen. Das gilt insbesondere für Cyber-Kriminelle, die es beispielsweise darauf anlegen, möglichst viele Systeme zum Teil eines sogenannten Botnetzes zu machen oder Zahlungsdaten für Online-Überweisungen von ihnen abzugreifen. Im Ergebnis setzen deutsche Behörden bereits heute Millionen Nutzerinnen und Nutzer von IT-Systeme weltweit, die von einer dem Staat bekannten Lücke betroffen sind, einem fortbestehenden Risiko von Cyber-Angriffen aus, um diese Sicherheitslücken im Einzelfall selbst für Maßnahmen nach §§ 100a Abs. 1 Satz 2 und 3, 100b StPO ausnutzen zu können. Das weltweite Missbrauchsrisiko, das hier durch ein Horten von Sicherheitslücken bewusst eingegangen wird, steht in keinem Verhältnis zu dem verfolgten Zweck, nämlich der (möglicherweise) erleichterten Strafverfolgung im Einzelfall.

Dass die Ausnutzung von staatlicherseits geheim gehaltenen Sicherheitslücken keine düstere Phantasie ist, hat der Vorfall um „WannaCry“ gezeigt: In den Abendstunden des 12. Mai 2017 machte sich dieses Schadprogramm, ein sog. Kryptotrojaner, auf den Weg. Innerhalb weniger Stunden waren weltweit etwa 220.000 Systeme betroffen. Der Trojaner verschlüsselte die Daten auf

den betroffenen Computern und bot den Nutzern zeitgleich einen Code für die Entschlüsselung an, ansonsten werde die Löschung der Daten veranlasst. In Deutschland war vor allem die Deutsche Bahn betroffen. In Großbritannien traf es das Gesundheitssystem besonders schwer. Zahlreiche Rechner des National Health Service waren befallen, manches Krankenhaus musste daraufhin Patienten abweisen. Der WannaCry-Trojaner nutzte eine Lücke im Betriebssystem Microsoft Windows. Diese Lücke war schon Jahre zuvor von der National Security Agency, des auf Hacking spezialisierten US-Geheimdienstes, entdeckt, aber nicht an den Hersteller Microsoft gemeldet worden. Brad Smith, Präsident von Microsoft, erhob den Vorwurf, die Geheimdienste würden diese Lücken absichtsvoll horten, statt sie sofort an die Hersteller zu melden.

Angesichts dieser Erfahrungen bekommen die eindringlichen Worte des Bundesverfassungsgerichts in seinem Urteil vom 27. Februar 2008 („Online-Durchsuchung“) erschreckende Aktualität:

„Je nach der eingesetzten Infiltrationstechnik kann die Infiltration auch weitere Schäden verursachen, die im Zuge der Prüfung der Angemessenheit einer staatlichen Maßnahme mit zu berücksichtigen sind. Wird dem Betroffenen etwa eine Infiltrationssoftware in Form eines vermeintlich nützlichen Programms zugespielt, lässt sich nicht ausschließen, dass er dieses Programm an Dritte weiterleitet, deren Systeme in der Folge ebenfalls geschädigt werden. Werden zur Infiltration bislang unbekannte Sicherheitslücken des Betriebssystems genutzt, kann dies einen Zielkonflikt zwischen den öffentlichen Interessen an einem erfolgreichen Zugriff und an einer möglichst großen Sicherheit informationstechnischer Systeme auslösen. In der Folge besteht die Gefahr, dass die Ermittlungsbehörde es etwa unterlässt, gegenüber anderen Stellen Maßnahmen zur Schließung solcher Sicherheitslücken anzuregen, oder sie sogar aktiv darauf hinwirkt, dass die Lücken unerkannt bleiben. Der Zielkonflikt könnte daher das Vertrauen der Bevölkerung beeinträchtigen, dass der Staat um eine möglichst hohe Sicherheit der Informationstechnologie bemüht ist.“ (BVerfGE 120, 274 <325 f.>)

Dieser Zielkonflikt mag für eine Ermittlungsbehörde bestehen. Für den Gesetzgeber aber, der dem Allgemeinwohl verpflichtet ist, muss die Sicherheit informationstechnischer Systeme Vorrang haben. Die in §§ 100a Abs. 1 Satz 2, 100b StPO geschaffenen Regelungen sind deshalb mit dem IT-Grundrecht nur dann vereinbar, wenn sie um ein Verbot ergänzt werden, bisher unbekannte Sicherheitslücken (sog. 0days) auszunutzen, solange der Hersteller des Systems nicht über die Lücke informiert ist. Eine Sicherheitslücke hingegen, die dem Hersteller bekannt ist, die aber beispielsweise wegen Nachlässigkeit des Systembetreibers noch nicht geschlossen wurde, kann auch aus der Perspektive der IT-Sicherheit ausgenutzt werden. Gleiches gilt für Sicherheitslücken, die nicht auf Fehlern der Hersteller beruhen, sondern auf einer individuellen fehlerhaften Einrichtung des informationstechnischen Systems. Aus diesem Grunde beeinträchtigt das Verbot des Ausnutzens von 0days auch die Interessen der

Sicherheitsbehörden nur unwesentlich, stehen ihnen doch gleichwohl mannigfaltige Wege zur Infektion von IT-Systemen zur Verfügung.

Die Bf. der von der GFF koordinierten Verfassungsbeschwerde erhoffen sich vom BVerfG im Sinne der vorstehenden Überlegungen eine Weiterentwicklung des IT-Grundrechts. Das Gericht sollte die objektiv-rechtlichen Dimension des IT-Grundrechts anerkennen und dem Gesetzgeber aufgeben, ein Regime zur angemessenen Behandlung von IT-Sicherheitslücken einzuführen. Kernbestandteil einer solchen Regelung muss das Verbot sein, 0days für hoheitliche Zwecke zu horten, statt sie schließen zu lassen.
