Aufzeichnungen vom Treffen mit Anwalt Dr. Peter Spengler zum Thema Verfassungsbeschwerde gegen den Hessentrojaner.

Montag, 28.01.2019

1. Fassung: Annette Schaper-Herget
Überarbeitung von Dr. Spengler

Teilnehmer, Dr. Spengler, Helge Herget, Dr. Annette Schaper-Herget und drei IT-Experten

Verteiler: alle Teilnehmer des Treffens, Vorstand Piratenpartei Hessen, Mitglieder der Chatgruppe Hessentrojaner (Telegram)

Dr. Spengler erläuterte seinen geplanten Argumentationsstrang:

Die Grundlage und Randbedingungen der Beschwerde
Gesellschaftliche Aktivitäten verlagern sich zunehmend ins Internet, damit auch alle Forment der Kriminalität. Die Polizei braucht daher irgendwelche Mittel, um die Sicherheit der Bürger auch im Internet zu gewährleisten und Bedrohungen abzuwenden. Wir können also nicht erwarten, dass das Bundesverfassungsgericht jegliche Internet-Aktivitäten der Polizei verbieten wird. Vielmehr hat das Gericht in seinen bisherigen Entscheidungen (von „Online-Durchsuchung“, 2008, bis „BKA-Gesetz“, 2016) deutlich gemacht, dass die heimliche Infiltration eines IT-Systems, um dieses zu überwachen und Speichermedien auszulesen, unter bestimmten Voraussetzungen verfassungsrechtlich zulässig ist.

Was aber genauer geklärt werden muss.
Das Bundesverfassungsgericht entnimmt Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz (allgemeines Persönlichkeitsrecht, Schutz und Achtung der Menschenwürde) das *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (IT-Grundrecht).* Die Infiltration eines IT-Systems durch Polizei- oder Verfassungsschutzbehörden bedarf als Eingriff in den Schutzbereich des IT-Grundrechts einer tragfähigen verfassungsrechtlichen Rechtfertigung. Die bisherige Rechtsprechung beschäftigte sich im Wesentlichen mit den Maßstäben hierfür. Schon weitgehend geklärt sind hiernach die Eingriffsvoraussetzungen unter den Gesichtspunkten der hinreichenden Bestimmtheit gesetzlicher Befugnisnormen, die wie § 15c HSOG eine Infiltration von IT-Systemen erlauben, der Verhältnismäßigkeit der Eingriffe und derer rechtsstaatlichen Kontrolle.
Die Bestimmungen des § 15c HSOG sind an diesem Stand der Rechtsprechung ausgerichtet. Grundlegende Korrekturen hinsichtlich der darin geregelten Eingriffsschranken werden nicht zu erreichen sein.
Das Grundgesetz schützt jedoch nicht nur vor Eingriffen des Staates in das jeweilige Grundrecht. Aus den Grundrechten folgen auch Schutzpflichten des Staates gegenüber Bedrohungen von Dritter Seite. Hiervon ausgehend kommt dem Grundrecht auf *Gewährleistung* der Vertraulichkeit und Integrität informationstechnischer Systeme auch die Bedeutung zu, dass der Staat „für IT-Sicherheit sorgen“ muss.

Daher stellt sich die Frage nach der verfassungsrechtlichen Einhegung eines auf das Offenhalten von Sicherheitslücken der IT-Infrastruktur angewiesenen Einsatzes informationstechnischer Aufklärungsmittel durch den Staat, hier die hessischen Polizeibehörden. Das Bundesverfassungsgericht identifizierte bereits in der Entscheidung „Online-Durchsuchung“ zum

nordrhein-westfälischen Verfassungsgesetz von 2006 den *Zielkonflikt zwischen den öffentlichen Interessen an einem erfolgreichen Zugriff und an einer möglichst großen Sicherheit informationstechnischer Systeme.*

Dieser Zielkonflikt ist Gegenstand von naturgemäß weder auf Hessen noch etwa auf Deutschland oder Europa beschränkten technischen, politischen und juristischen Diskussionen. Zufriedenstellender Auflösung harrt er auf allen Ebenen.
Hiervon ausgehend ließe sich der verfassungsrechtliche Standpunkt einnehmen, der einzelne Grundrechtsträger könne als Verletzung eines aus dem IT-Grundrecht folgenden Schutzanspruchs rügen, dass der Staat gesetzliche Voraussetzungen für Eingriffe in informationstechnische Systeme schafft, ohne dies an ein irgendwie adäquates Sicherheits- und Schwachstellenmanagement zu knüpfen. Einen solchen Ansatz verfolgen die von Prof. Singelnstein vertretenen Verfassungsbeschwerden gegen § 23b Abs. 2 des baden-württembergischen Polizeigesetzes von 2017.

Dieser Ansatz hat insoweit ein großes Erfolgspotenzial, als der objektive Zielkonflikt nicht von der Hand zu weisen ist und eine Entschärfung durch Regelungen über ein Schwachstellenmanagement, aber etwa auch zur Betätigung der Sicherheitsbehörden auf dem „Beschaffungsmarkt“ für Sicherheitslücken durchaus vorstellbar ist und geboten erscheint. Nicht ohne Weiteres zwingend ist die Verknüpfung einer darauf gerichteten staatlichen Handlungspflicht mit einem konkreten individuellen Schutzanspruch des einzelnen Grundrechtsträgers.

Die staatlichen Schutzpflichten in Bezug auf die IT-Sicherheit sind jedoch Gegenstand einer wichtigen juristischen Diskussion, die in der Literatur zu dem IT-Grundrecht auch schon seit längerer Zeit eröffnet ist, und die neueren Vorschriften über Staatstrojaner bieten jedenfalls Gelegenheit für den Versuch, über Individualverfassungsbeschwerden zur Klärung und Weiterentwicklung der verfassungsrechtlichen Maßstäbe durch das Bundesverfassungsgericht beizutragen.

Eine Argumentation für die Verfassungsbeschwerde gegen § 15c HSOG lässt sich demnach so skizzieren:

Der Staat will Sicherheitslücken nutzen, also kann man ein „Schwachstellenmanagement“ verlangen, das die Sicherheit der Bürger gewährleistet. Man kann zwar nicht im Detail vorschreiben, wie ein solches Schwachstellenmanagement im Detail aussieht, aber man kann fordern, dass ein solches erstellt wird. Denn man kann bemängeln, dass das in der derzeitigen Gesetzesfassung unzureichend geregelt ist und dass unerwünschte Nebenwirkungen, wie die Korrumpierung von IT-Systemen, nicht ausgeschlossen werden können.

Also kann man fordern, dass folgendes genauer geregelt wird:

- die rechtlichen Voraussetzungen, wann die Polizei einen Trojaner anwenden darf
- die technischen und rechtlichen Umstände, unter denen er eingesetzt werden darf
- wie die Informationspflicht für die Betroffenen gehandhabt wird (sobald der Betroffene davon erfährt, ist die teuer eingekaufte Sicherheitslücke kompromittiert)
- wie dafür gesorgt werden soll, dass dass Offenhalten der Sicherheitslücke nicht andere IT-Strukturen korrumpiert, nach dem Beispiel von „Wannacry“
- wie sichergestellt werden kann, dass von einem Trojaner keine Gefährdung ausgeht
- Wie die Beschaffungsmaßnahmen der Sicherheitslücken vonstatten gehen sollen
- welche konkreten Mittel eingesetzt werden sollen
- wo die rechtsstaatlichen Schranken liegen, um Verhältnismäßigkeit zu gewährleisten.

Also, zusammenfassend: die Rahmenbedingungen müssen kleinteiliger geregelt werden.

Bitte an die IT-Experten:
Spengler bittet darum, ihm Quellen und Literatur zum Umgang mit Sicherheitslücken und nach Möglichkeit auch zu deren „Beschaffung“ durch die (hessichen) Polizeibehörden zur Verfügung zu stellen, die er in der Beschwerde zitieren kann, und an die er anschließen kann. Bitte auch für Nicht-Informatiker verständlich. Also Darstellungen der Problematik von Sicherheitslücken, Literatur zum Entwicklungsstand von Schwachstellenmanagement. Wie sieht die Realität aus, bezüglich Eindämmung von Trojanern und Missbrauch von Sicherheitslücken?

IT-Experte:
Zur Verhältnismäßigkeit: In den meisten Fällen würden Beschlagnahmungen von PCs und Handys ausreichend, Trojaner wäre unverhältnismäßig. Und zur Gefahrenabwehr ist Quellen-TKÜ viel zu langsam.
Bisher gibt es kaum Vorschriften, zur Zeit gibt es wohl höchstens eine Richtlinie im BKS.
Allein dadurch, dass man so etwas aufspielt, kann man zeigen, dass ein System korrumpierbar ist.
Die Variante, dass jemand von aussen über das Internet zugreift, ist eher die Ausnahme, eher passiert das über zugespielte Datenträger.
Sicherheitslücken werden von eingetragenen Firmen gehandelt, unter Ausschluss der Hersteller.
Wahrscheinlich ist limitiert, wer dort einkaufen darf.

Noch mal zum Thema Beschwerdeführer:
In den anderen Beschwerden werden immer Leute gewählt, die „ganz besonders betroffen“ sind, also z.B. Anwälte oder Journalisten, die kritisch aus totalitären Staaten berichten. Aber warum sollten ein Büger stärker geschützt werden als ein anderer? Alle haben das gleiche Recht, geschützt zu werden. Trotzdem wäre es als „Fallback“, um die Erfolgsaussichten zu steigern, zu überlegen, noch einen Beschwerdeführer zu finden, der „ganz besonders betroffen“ ist.
Dies habe ich neulich mit den Datenschützern Rhein/Main diskutiert, die auch diesen Vorschlag gemacht haben. Ich werde bei denen anfragen, ob sie jemanden vorschlagen können.

Nächste Schritte:
- Die IT-Experten suchen passende Literatur
- Ich diskutiere das im Hessenvorstand und frage bei den Datenschützern Rhein-Main nach.
- Dr. Spengler sagt, dass der Trojaner bei ihm jetzt die höchste Priorität hat und wir im Februar mit einer ausgearbeiteten Beschwerdeschrift rechnen können.

Nachtrag:
Inzwischen haben die IT-Experten uns eine umfangreiche Literaturliste überlassen.