CCCS gegen erneute Verschärfung des Polizeigesetzes

Seit einigen Tagen kursiert der Entwurf des Innenministeriums für eine erneute Änderung des erst Ende 2017 beschlossenen Polizeigesetzes (PolG) in Baden-Württemberg. Bei dem bereits verabschiedeten PolG handelt es um eines der schärfsten in Deutschland. Die nun angedachte, abermalige Ausweitung polizeilicher Befugnisse soll offenbar die Lücke zum traurigen Spitzenreiter Bayern mit dessen viel kritisierten Polizeiaufgabengesetz schließen. Jedoch kann das Innenministerium weder die Wirksamkeit der letztjährigen Verschärfung belegen, noch einen Nachweis für die Notwendigkeit dieser erneuten Änderungen bieten. Die geplanten Neuerungen wie Gewahrsam für Unschuldige, willkürliche Durchsuchungen von Menschen bei großen Veranstaltungen (z.B. Demonstrationen), DNA-Analyse zur Erstellung eines genetischen Fingerabdrucks, Bodycams auch in Gebäuden und vieles mehr halten wir für sehr bedenklich. Gerade die Ausweitung von polizeilichen Befugnissen weit ins Vorfeld einer möglicherweise geplanten Straftat (und somit auf völlig Unschuldige) werden das bisher gute Verhältnis zwischen BürgerInnen und ihrer Polizei nachhaltig beschädigen.

Dies alles soll jedoch nicht Kern dieser Veröffentlichung sein. Vielmehr wollen wir dezidiert auf die geplante „Online-Durchsuchung“, also das Infizieren von Endgeräten (Laptops, Smartphones u.ä.) mit staatlicher Schadsoftware eingehen. Dies geschieht mit der Absicht, deren Speicher und die Daten der installieren Apps und Programme auszulesen, oder die Geräte zu einem Peilsender zur Überwachung des Standorts umzufunktionieren.

Der Chaos Computer Club Stuttgart widerspricht der Einführung einer solchen Maßnahme entschieden. Die vielen Probleme und Gefahren durch die 2017 beschlossene „Quellen-Telekommunikations-Überwachung“ treten bei der „Online-Durchsuchung“ verschärft zu Tage:

- Um die Schadsoftware unbemerkt und zuverlässig auf ein Gerät aufbringen zu können, werden dem Hersteller des Produkts **unbekannte Sicherheitslücken** benötigt. Auch nach deren Auffinden (oder deren Einkauf aus meist zweifelhaften Quellen) können diese Lücken **nicht an den Hersteller gemeldet** werden, da diese sonst geschlossen würden und somit als Infektionsweg unbrauchbar würden. In einer Welt, in der Computer zunehmend in jedem Bereich eingesetzt werden, muss deren Absicherung **oberste Priorität** haben. Das Festhalten am **Konzept des Staatstrojaners ist die systematische Verunsicherung der deutschen IT-Landschaft**, sie hat den entgegengesetzten Effekt und gefährdet somit Privatpersonen, Firmen und Infrastruktur. Auch und gerade die in Baden-Württemberg ansässigen kleinen und mittleren Unternehmen (KMU) sind mehr denn je auf möglichst sichere IT angewiesen, ihnen fehlen schlicht die Mittel für gut ausgestattete IT-Sicherheits-Abteilungen. Dass die Bedrohung durch staatlich gewolltes Offenhalten von Lücken real ist, hat spätestens die weltweite Ausbreitung der Schadsoftware WannaCry vor gut einem Jahr bewiesen[1]. **Die Gefahr**, die von solchen gravierenden Sicherheitslücken für die

1 https://de.wikipedia.org/wiki/WannaCry

Bevölkerung ausgeht, **ist deutlich größer** (z.B. Ausfall eines Krankenhauses[2]) **als der angebliche und unbewiesene Nutzen** für die Sicherheitsbehörden[3].

- Gleichzeitig schwächt dieser **innere Konflikt** in der Zielsetzung staatlichen Handelns (sichere Systeme vs. Zugriffsmöglichkeit auf jedes Gerät) zwangsläufig die vorhandenen institutionellen Bemühungen für mehr IT-Sicherheit, da diese in letzter Konsequenz gegen die Sicherheitsbehörden arbeiten müssten. Leidtragende sind die Bevölkerung, die Wirtschaft und, durch unsicherere Systeme, auch der Staat selbst.

- Ein weiteres Dilemma besteht in der Tatsache, dass deutsche Behörden in der Vergangenheit massive Probleme hatten, selbst geeignete Software zu erstellen. Dies wurde und wird durch **Zukauf von kommerziellen Produkten** gelöst. Sollte dies auch in BW der Fall sein, muss sicher gestellt sein, dass diese Lieferanten nicht auch parallel in repressive Regime exportieren[4] oder der begründete Verdacht darauf besteht.

- Auf dem Zielgerät solch eines digitalen Einbruchs werden zwangsläufig wichtige Sicherheitsfunktionen deaktiviert, um das Auslesen von Daten zu ermöglichen. Dies führt in unseren Augen in der Folge dazu, dass von solch einem Gerät **gewonnen Beweise** als **nicht vertrauenswürdig** einzustufen sind. Welcher Richter würde Beweise aus der Durchsuchung einer Wohnung verwerten, bei der zuvor Wochen lang die Türe offen stand?

- Sowohl bei der „Quellen-TKÜ“ als auch bei der „Online-Durchsuchung“ wird praktisch **zwangsläufig** auch **Kommunikation aus dem strikt zu schützenden Kernbereich privater Lebensführung erfasst**. Dies kann im Vorfeld technisch nicht verhindert werden und schließt solch eine Maßnahme, aus unserer Sicht, prinzipiell aus.

- Das Smartphone erfüllt für immer mehr Menschen die Funktion eines „**ausgelagerten Gehirns**“, dies hat auch das Bundesverfassungsgericht festgestellt[5]. Unsere Geräte sollten deshalb (wie auch unsere Gedanken) **unbedingten Schutz** genießen.

Auch unabhängig von diesen prinzipiellen Gründen gegen Staatstrojaner hat der vorliegende Entwurf des neuen Polizeigesetzes erhebliche Mängel:

- Es sind keine **Qualitätsanforderungen** an die verwendete Soft- und ggf. Hardware definiert. Diese Vorgaben müssen, der Schwere des Eingriffs angemessen, höchsten Anforderungen genügen und sind dem Landesdatenschutzbeauftragten im Vorfeld vorzulegen.
- Eine **unabhängige Prüfung** der verwendete Soft- und ggf. Hardware durch den Landesdatenschutzbeauftragten und ggf. durch von ihm hinzu gezogene ExpertInnen, die auch den Quellcode umfasst, ist nicht vorgesehen.
- Eine **Informationspflicht** gegenüber den Betroffenen nach Abschluss der Maßnahme ist nicht vorgesehen.

2 https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack
3 https://cdn.netzpolitik.org/wp-upload/2018/09/2018-07-02_Frank-Kuhn_Bachelor_Gefaehrdet-Spionagesoftware-die-Innere-Sicherheit.pdf
4 https://en.wikipedia.org/wiki/FinFisher#Use_by_repressive_regimes
5 https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html

- Wie auch bei der (schon beschlossenen) „Quellen-TKÜ“ ist keine **unabhängige, wissenschaftliche Evaluation** vorgesehen. Die Evaluierungsphase darf, aus unserer Sicht, nicht länger als 12 Monate betragen. Die Ergebnisse sind neben dem Landtag auch der Bevölkerung zugänglich zu machen.

Zusammenfassend fordert der CCCS:

1. Keine Möglichkeit zur „Online-Durchsuchung“ im neuen PolG
2. Rücknahme der bereits beschlossenen Möglichkeit zur „Quellen-TKÜ“
3. Sofortige Meldepflicht von durch staatlichen Stellen gefundene Sicherheitslücken
4. Feste Integration des Themas IT-Sicherheit in Ausbildung und Lehre
5. Einen Topf von 2 Millionen € p.a. als Belohnung für das Melden von bisher unbekannten Sicherheitslücken („Bug-Bounty-Programm“[6]) in weit verbreiteten Open-Source-Anwendungen

Ansprechpartner bzgl. dieser PM

Stefan Leibfarth
Signal/Mobil: 0172 63 43 48 0; E-Mail: leibi@cccs.de

6 https://de.wikipedia.org/wiki/Bug-Bounty-Programm