Sicherheit nicht gegen Datenschutz ausspielen!

Die Quellen-Telekommunikationsüberwachung, landläufig "Staatstrojaner" genannt, ist eine sicherheitspolitische Maßnahme, die die Gefahr birgt, auf lange Sicht zu mehr Unsicherheit als zu Sicherheit zu führen. Zugleich bedeutet die Anwendung von Staatstrojanern auf Computern, Smartphones und Tablets einen für die eigene Person nicht nachvollziehbaren und extremen Eingriff in die informationelle Selbstbestimmung und Privatsphäre. Die GRÜNE JUGEND Hessen setzt sich für eine Politik der Bürger*innenrechte ein und wird dies weiter konsequent tun. Wir wollen eine effektive Sicherheitspolitik, die sich an rechtstaatlichen Vorgaben orientiert!

Aus den folgenden Gründen halten wir eine Einführung von Staatstrojanern für eine Gefahr:

1. Auf Smartphones sind nahezu alle Informationen über eine Person gespeichert. Es können Bewegungsprofile, Gesundheitsprofile, private Bilder, Videos, Aufzeichnungen, alle Nachrichten und Beiträge abgegriffen werden. Staatstrojaner bzw. Quellen-TKÜ bedeutet vollen Zugriff auf diese Daten. Im Unterschied zur "klassischen TKÜ", bei der die Nachricht auf dem Übermittlungsweg abgefangen werden kann, muss bei der Quellen-TKÜ an die "Quelle" und dort abgespeicherte Inhalte gegangen werden. Dies liegt darin begründet, dass die Daten von Messengerdiensten "end-to-end" verschlüsselt übertragen werden (z.B. bei WhatsApp, Telegram). Um aber an die Quelle – und somit an die noch oder wieder unverschlüsselten Nachrichten – zu gelangen, muss der Staat auf den "Kernbereich" des technischen Gerätes mit vollen Administrator*innenrechten zugreifen, da die Bereiche sonst abgeschirmt werden. Damit besteht technisch notwendigerweise ein Vollzugriff auf die Quelle, d.h. alle Daten auf dem jeweiligen technischen Gerät können abgegriffen werden.
2. Um an die notwendige Technik und Programme zu gelangen, muss der Staat Dritte (private Firmen oder Auftragnehmer) beauftragen. Aus dem gleichen Grund kann der Staat aber auch nicht eigenständig kontrollieren, was der Trojaner macht und zu welchen Funktionen er fähig ist. Aufgrund der Auslagerung an Private kann sich der Staat und können die mit der Technik arbeitenden Sicherheitsbehörden sich auch nie sicher sein, die vollständige Kontrolle über die eingesetzte Software zu besitzen. Hier entsteht folglich eine strukturell unvermeidliche Kontroll- und Sicherheitslücke.
   Der Einsatz des bisherigen Bundestrojaners Anfang des Jahrzehnts hat genau diese Kontroll-und Sicherheitslücke und die Folgen offengelegt: Der Bundestrojaner, welcher 2011 vom CCC überprüft werden konnte versandte unverschlüsselt zuvor abgegriffene Daten. Er schaffte also aktiv Datenlecks, die neben der beauftragten Firma noch weitere Dritte hätten nutzen können. Diese Datenlecks entstanden auch in den Behörden, deren Befehle an den

Trojaner ebenfalls unsicher übermittelt wurden. Der Bundestrojaner schwächte also die Sicherheitsinfrastruktur von Behörden, anstatt mehr Sicherheit zu schaffen.

3. Um einen Trojaner auf ein Gerät aufzuspielen braucht es sog. Zero-Day-Exploits, also Sicherheitslücken in den betroffenen Programmen auf einem Gerät, z. B. im Betriebssystem eines Smartphones. Für diese Sicherheitslücken existiert bereits jetzt ein grauer bzw. schwarzer Markt. Dieser wurde und wird durch Staaten, die Sicherheitslücken "einkaufen", nur noch mehr gestärkt – zulasten der Verbraucher*innen und Endgerätnutzer*innen. Gleichzeitig verlieren staatliche Behörden das institutionelle Interesse daran, diesen Markt zu bekämpfen und Sicherheitslücken zu schließen. Die informationelle Sicherheit ("Cyber-Sicherheit") zu verbessern steht somit dem institutionellen Interesse von Polizei- und Geheimdiensten, welche mit Staatstrojanern arbeiten, entgegen. Staatstrojaner schwächen somit die Sicherheit von Informationssystemen. Die weltweit verheerende Schadsoftware Wannacry nutzte eine solche Lücke, deren Existenz vom US-Geheimdienst NSA verschwiegen und genutzt worden war.
   "Cybersicherheit" oder die Sicherheit informationeller Systeme ist essentiell. Bereits beim derzeitigen Stand der Digitalisierung war z. B. Wannacry nicht nur in der Lage, die IT-Infrastruktur zahlreicher Unternehmen und die zentrale Infrastruktur der deutschen Bahn zu beschädigen, sondern auch beispielsweise das Gesundheitssystems von Großbritannien, den NHS. Die Vernetzung und Digitalisierung wird absehbar weiter drastisch zunehmen. Damit steigt auch unweigerlich die Anfälligkeit aller Gesellschaftsbereiche für informationelle Attacken.
4. Wir als junge Menschen wollen Politik langfristig und damit auch unsere Zukunft gestalten. Langfristig stehen beim Thema Staatstrojaner dem kurzfristigen Sicherheitsgewinn einer vollständigen Durchleuchtung weniger sog. Gefährder*innen große Gefahren für alle im Zusammenhang mit der informationellen Sicherheit gegenüber. Deshalb ist eine staatliche Förderung von Sicherheitslücken, um als Staat Schadsoftware einsetzen zu können, eine Maßnahme, welche Sicherheit zwar vorgaukelt, aber de facto zu mehr Unsicherheit führen kann.
   Die Quellen-TKÜ stellt in ihrer sicherheitspolitischen Dimension auch einen Eingriff den Schutzbereich des Grundrechts der informationellen Selbstbestimmung aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG dar. Fraglich ist, ob und mit welchen Begründungen dieser Eingriff dann gerechtfertigt werden kann.
5. Wir sehen die akuten Bedrohungen und neuen Bedrohungsformen der Gesellschaft. Sowohl in rechten Kreisen, als auch in der islamistischen und salafistischen Szene wird der offenen Gesellschaft und den demokratischen und emanzipatorischen Errungenschaften der Kampf angesagt. Diesem gilt es sich - auch mit Hilfe der Sicherheitsbehörden - entgegenzustellen.

Dabei darf jedoch Sicherheit nicht gegen Datenschutz und durch Grundrechte garantierte Freiheiten ausgespielt werden. Die GRÜNE JUGEND Hessen befürwortet deswegen eine bessere personelle Ausstattung der Polizeibehörden, eine bessere technische Ausstattung und Ausbildung und die konsequente, an rechtsstaatlichen Prinzipien orientierte Durchführung der bereits gesetzlich im Hessischen Gesetz über die öffentliche Sicherheit und Ordnung verankerten Polizeimaßnahmen. Die weiteste Ausreizung des Grundgesetzes kann nicht Maßgabe grüner Sicherheitspolitik sein.

Die GRÜNE JUGEND Hessen sieht im Vorschlag für das Hessische Verfassungsschutzgesetz eine deutlich rechtsstaatlichere Version der Quellen-TKÜ. Der doppelte Richter*innenvorbehalt, der hier vorgesehen ist, wäre für die Bundesgesetze zum BKA dringend nötig. Aus den im Antrag beschriebenen Gründen sehen wir aber die Quellen-TKÜ generell kritisch. Sollte die Quellen-TKÜ in Hessen Bestandteil des Maßnahmenkatalogs der Sicherheitsbehörden werden, fordern wir zusätzlich ein Verbot von Zusammenarbeit mit Firmen, die ihre Systeme nicht nur an den Staat, sondern auch an autoritäre und totalitäre Systeme oder Gruppierungen liefern, um die Wirkungen der Quellen-TKÜ auf die Sicherheitsinfrastruktur abzumildern.

Beschlossen am 05.11.2017 auf der Landesmitgliederversammlung in Limburg an der Lahn.