327/J
vom 20.12.2024 (XXVIII. GP)

Anfrage

der Abgeordneten David Stögmüller, Freundinnen und Freunde

an den Bundesminister für Inneres

betreffend Beschaffung von Spionagesoftware

BEGRÜNDUNG

2018 wurde durch die damalige Schwarz-Blaue Regierung ein neues Gesetz verabschiedet, das den Einsatz von Spionagesoftware durch staatliche Behörden erlaubte, der sogenannte „Bundestrojaner". Diese Software hätte es den Strafverfolgungsbehörden ermöglicht, in Ermittlungsverfahren auf Daten von Zielpersonen zuzugreifen, indem Überwachungssoftware auf deren Geräte gespielt wird. Mit diesem Gesetz sollten terroristische Bedrohungen und organisierte Kriminalität bekämpft werden. Im Dezember 2019 erklärte jedoch der Verfassungsgerichtshof dieses Gesetz als verfassungswidrig und hob es auf (Erkenntnis vom 11.12.2019, G 72-74/2019, G 181-182/2019)[1]. Die Verfassungsrichter sahen in der damaligen Regelung gravierende Eingriffe in Grundrechte wie den Schutz der Privatsphäre, welche nicht ausreichend durch Kontrollmechanismen abgesichert waren.

Im August 2024 wurde nun ein neuer Gesetzesentwurf des ÖVP-geführten Innenministeriums in die Begutachtung geschickt, der neuerlich die Überwachung verschlüsselter Nachrichten auf Handys erlauben soll[2]. Wir Grüne haben weiterhin erhebliche Bedenken bezüglich dieses Entwurfs, insbesondere in Bezug auf den verfassungsrechtlichen Schutz der Grundrechte, die durch die Begutachtung nicht ausgeräumt wurden.

Auch das Europäische Parlament hat sich mit dieser Thematik beschäftigt und in seiner Untersuchung der Spionagesoftware Pegasus festgestellt, dass diese von verschiedenen europäischen Staaten eingesetzt wurde, um nicht nur Kriminelle und Terroristen zu überwachen, sondern auch Journalist:innen, Oppositionelle und Anwält:innen. Solche Praktiken stellen eine ernste Bedrohung für die Demokratie und den Schutz der Zivilgesellschaft dar. In seinem Abschlussbericht äußerte der Untersuchungsausschuss des Europäischen Parlaments Bedenken über die negativen Auswirkungen des Missbrauchs von Spionagesoftware auf die Demokratie, die Zivilgesellschaft und die Pressefreiheit in mehreren EU-Mitgliedstaaten.[3] Diese Bedenken sind auch im vorliegenden Fall von großer Relevanz, da nicht ausgeschlossen

[1] https://www.vfgh.gv.at/medien/Kfz-Kennzeichenerfassung_und_Bundestrojaner_verfass.de.php
[2] https://www.parlament.gv.at/gegenstand/XXVII/ME/350?selectedStage=100
[3] https://www.europarl.europa.eu/news/de/agenda/briefing/2023-06-12/2/untersuchung-zu-pegasus-spahsoftware-abgeordnete-skizzieren-notwendige-reformen

werden kann, dass ähnliche Überwachungspraktiken in Österreich durch den Einsatz solcher Software möglich werden könnten.

Neben grundrechtlichen Bedenken, stellt sich aber auch die Frage, wie diese Software beschafft werden soll, von welchem Anbieter sie programmiert wird und welche Verbindungen diese Anbieter zu ausländischen, insbesondere russischen, Akteuren haben könnten. Gefüttert werden diese Bedenken auch dadurch, dass der abgebrochene Beschaffungsprozess der Software auf Basis des Gesetzes 2018 weiterhin komplett geheim gehalten wird.

In anderen Ressorts gibt es konkrete Anhaltspunkte dafür, dass diese Bedenken nicht vom Tisch geräumt werden können. Ein Beispiel hierfür ist der Beschaffungsprozess, den das Bundesministerium für Landesverteidigung (BMLV) mit der Firma DSIRF einleitete, um eine Spionagesoftware zu testen. Diese Firma stand nicht nur im Verdacht, enge Verbindungen nach Russland zu unterhalten, sondern möglicherweise auch zu Jan Marsalek, dem ehemaligen Wirecard-Vorstand, der wegen schwerer Wirtschaftsdelikte international gesucht wird und der verdächtigt wird, einen russischen Spionagering aufgebaut zu haben.[4] Solche Verbindungen werfen erhebliche Fragen nach der Integrität und Sicherheit der Software auf, die von solchen Firmen bereitgestellt wird, insbesondere wenn diese tief in die IT-Infrastruktur und Kommunikationssysteme der österreichischen Bevölkerung eingreifen sollen. Es ist daher politisch von höchster Relevanz, Transparenz über die Herkunft und Funktionsweise der einzusetzenden Software sicherzustellen.

Ein weiterer kritischer Punkt ist die Möglichkeit, dass Sicherheitslücken, die für die Implementierung der Software genutzt werden, von Firmen mit zweifelhaftem Ruf bereitgestellt werden. Diese Firmen arbeiten oft nicht nur mit europäischen Sicherheitsbehörden, sondern auch mit autoritären Regimen zusammen, die solche Techniken zur Unterdrückung der Zivilbevölkerung und der Opposition verwenden. Vor diesem Hintergrund ist es von entscheidender Bedeutung, detaillierte Informationen darüber zu erhalten, welche Anbieter in Betracht gezogen werden und welche Sicherheits- und Kontrollmechanismen geplant sind, um einen Missbrauch der Technologie zu verhindern.

Die unterfertigenden Abgeordneten stellen daher folgende

ANFRAGE

1) Ich ersuche um Übermittlung aller Dokumente des damaligen Vergabeverfahrens an den Unterausschuss des Ausschusses für Innere Angelegenheiten des Nationalrats.
2) Wie erfolgte das öffentliche europäische Auswahlverfahren zur Anschaffung einer Spionagesoftware nach in Kraft treten des Gesetzes 2018?
   a) Wann wurde es eingeleitet?

[4] https://www.profil.at/oesterreich/bundesheer-tarnen-und-taeuschen-um-spionagesoftware/402357828

b) Wann wurde es eingestellt?
c) Welche gesonderten Richtlinien gibt es in der Zusammenarbeit mit Unternehmen für diesen besonders grundrechtsrelevanten aber auch sicherheitskritischen Bereich?
   i) Wenn es keine gesonderten Richtlinien gibt, warum nicht und welche anderen Richtlinien werden in diesen Prozessen angewendet?
   ii) Wenn es keine gesonderten Richtlinien gibt, werden diese für zukünftige Anschaffungen ausgearbeitet?
d) Mit welchen Anbietern wurden im Zuge dieses Verfahrens Gespräche geführt und welche Dokumente oder Informationen wurden von diesen übermittelt?
e) Wo genau wurde dieses Auswahlverfahren veröffentlicht?
f) Wie wurden die Anbieter ermittelt und ausgewählt?
   i) Von welchen europäischen Organisationseinheiten wurden Erfahrungswerte eingeholt? Welche Erfahrungswerte wurden hier geteilt?
g) Welche Anbieter wurden zur Legung von Angeboten eingeladen?
h) Welchen Sicherheitskriterien und/oder Richtlinien unterlagen die eingeladenen Anbieter?
   i) Wie wurde deren Hintergrund geprüft?
   ii) Wie sieht eine Eignungsprüfung für Unternehmen/Anbieter für eine solche Beschaffung genau aus?
   iii) Werden Verbindungen zu Russland, China oder den Iran aktiv überprüft?
i) Wie viele Angebote aus der Ausschreibung liegen dem Bundesministerium f. Inneres vor?
j) Wurde eine bestimmte Software angestrebt, die bereits von anderen Ministerien geprüft wurde?
   i) Wurde der Einsatz der Software der Firma DSIRF, die durch das Bundesministerium für Landesverteidigung getestet wurde, geprüft?
k) Wie hoch waren die Kosten der einzelnen Angebote für die Beschaffung der Software?
l) Wurde im Beschaffungsverfahren die Offenlegung des Quellcodes gefordert, um die Anwendung in der Strafverfolgung nachvollziehbar zu machen?
   i) Wenn nein, warum nicht?
   ii) Wird eine solche Offenlegung in Zukunft gefordert werden? Wenn nein, warum nicht?

3) Mit den Erfahrungswerten des Beschaffungsvorgangs 2018, welche Kosten erwarten sie für eine Anschaffung einer zukünftigen Software auf Basis des am 14.8.2024 in Begutachtung geschickten Ministerialentwurfs (350/ME) zur Änderung des Staatsschutz- und Nachrichtendienstgesetzes?
4) Mit den Erfahrungswerten rund um die Überwachung von Journalist:innen, Anwält:innen und Oppositionellen durch die Spioange-Software Pegasus, werden sie besondere Vorkehrungen in einer zukünftigen Software verlangen, damit keine Überwachung der obengenannten Personengruppen möglich ist?
5) Laut dem Entwurf soll eine Überwachung auf laufende Messenger-Kommunikation beschränkt werden und keinen Komplett-Zugriff ermöglichen. Gem § 15 a Abs 5 ist technisch sicherzustellen, dass 1. ausschließlich innerhalb des Bewilligungszeitraums gesendete, übermittelte oder empfangene Nachrichten überwacht werden können, 2. an dem zu überwachenden Compu-

tersystem nur Veränderungen vorgenommen werden, die für die Nachrichtenüberwachung unerlässlich sind, und 3. das eingebrachte Programm nach Beendigung der Ermittlungsmaßnahme entfernt oder funktionsunfähig wird. Ausdrücklich wird in den Erläuterungen festgehalten: „Die einzubringende Software ist technisch regulierbar, sodass nur gezielte und von der Bewilligung umfasste Nachrichten aus bestimmten Applikationen ausgeleitet werden können". In der Begutachtung wurde in mehreren Stellungnahmen ausgeführt, dass eine derartige technische Spezifikation nicht möglich ist.

   i) Gibt es konkrete Angebote, die diese technischen Spezifikationen erfüllen?
   ii) Wenn ja, wer hat diese Angebote gestellt?
   iii) Wie sollen die in den Erläuterungen dargestellten Beschränkungen sichergestellt werden?
   iv) Gibt es dazu konkrete Machbarkeits-Analysen?
   v) Wenn ja, wer hat diese Analysen durchgeführt?

6) Wie soll sichergestellt werden, dass Sicherheitslücken in Endgeräten, die für die Einbringung der Überwachungssoftware genutzt werden sollen, nicht von Geheimdiensten und ausländischen Regierungen oder kriminellen Organisationen genutzt werden können? Gibt es ein Software-Angebot, das hier eine technisch nachvollziehbare Lösung beinhaltet?
   i) Wenn ja, wer hat dieses Angebot gestellt?
7) Wie soll die gesetzlich vorgesehene Spezifikation für die Überwachungssoftware überprüft werden. Ist eine Zertifizierung durch eine unabhängige Stelle vorgesehen?
   i) Welche Zertifizierungsstelle soll das sein?

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2024-12-20T14:33:21+01:00
Prüfinformation	Dieses Dokument wurde elektronisch besiegelt. Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel	