MINISTERIUM DES INNEREN, FÜR DIGITALISIERUNG UND KOMMUNEN
B A D E N - W Ü R T T E M B E R G

Postfach 10 34 65 • 70029 Stuttgart
E-Mail: poststelle@im.bwl.de
FAX: 0711/231-5000

An die
Präsidentin des Landtags
von Baden-Württemberg
Frau Muhterem Aras MdL
Haus des Landtags
Konrad-Adenauer-Str. 3
70173 Stuttgart

Datum 23.08.2021

nachrichtlich
Staatsministerium

Antrag des Abgeordneten Nico Weinmann u. a. FDP/DVP
- Einsatz der Spyware „Pegasus“ in Baden-Württemberg
- Drucksache 17/652
Ihr Schreiben vom 30.07.2021

Sehr geehrte Frau Landtagspräsidentin,

das Ministerium des Inneren, für Digitalisierung und Kommunen beantwortet den Antrag wie folgt:

1. *welche Kenntnisse sie über den Einsatz der Spyware „Pegasus“ und Betroffene dadurch erfolgter Überwachung in Baden-Württemberg allgemein hat?*

Zu 1.:

Es liegen keine über die öffentlich verfügbaren Informationen hinausgehenden Erkenntnisse zum Einsatz der Spyware „Pegasus“ vor. Eine gesonderte Betroffenheit von Personenkreisen in Baden-Württemberg ist nicht bekannt.

2. *welche Maßnahmen sie im Einzelnen ergriffen hat, um den Einsatz der Spyware „Pegasus“ durch beziehungsweise gegen Bürgerinnen und Bürger aus Baden-Württemberg zu erforschen?*

Zu 2.:

Die zuständigen Stellen im Land analysieren die Entwicklung der Lage aufmerksam und stehen hierzu untereinander und mit den Sicherheitsbehörden des Bundes in engem Austausch.

Durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) erfolgte am 27. Juli 2021 die Veröffentlichung eines Warnhinweises vor einer möglichen Überwachung mittels „Pegasus“. Die Warnmeldung wurde durch die Medienberichterstattung aufgegriffen und damit der breiten Öffentlichkeit zugänglich gemacht.

3. *ob sie oder Behörden des Landes Baden-Württemberg, wie das Landeskriminalamt oder das Landesamt für Verfassungsschutz „Pegasus“ selbst einsetzen, dies planen oder entsprechende Gespräche mit dem Hersteller geführt haben?*

Zu 3.:

Zu Einzelheiten der informationstechnischen Überwachung durch die Sicherheitsbehörden können grundsätzlich keine öffentlich zugänglichen Auskünfte erteilt werden. Informationen im Zusammenhang mit Einsatzmitteln, Produkten oder Herstellern im Bereich der informationstechnischen Überwachung sind besonders geheimhaltungsbedürftig, weil sie bei Bekanntwerden weitgehende Rückschlüsse auf die Arbeitsweise und Methoden der Sicherheitsbehörden zulassen würden, wodurch deren Funktionsfähigkeit beeinträchtigt und in der Folge auch die Sicherheit des Landes in erheblicher Weise gefährdet werden könnte. Die vorstehenden Ausführungen gelten unabhängig davon, ob das im Einzelfall angefragte Produkt eingesetzt wird oder nicht.

Aus der Abwägung der verfassungsrechtlich garantierten Informationsrechte der Abgeordneten mit den negativen Folgen für die künftige Arbeit und Aufgabenerfüllung der Sicherheitsbehörden sowie den daraus resultierenden Beeinträchtigungen der Sicherheit des Landes Baden-Württemberg folgt, dass der Erkenntnisstand nur in einem

gesonderten „VS-NUR FÜR DEN DIENSTGEBRAUCH“ eingestuften Antwortteil dargestellt werden kann, auf den hiermit verwiesen wird.

4. *ob ihr bekannt ist, ob andere deutsche Sicherheitsbehörden des Bundes oder anderer Länder, wie insbesondere das Bundeskriminalamt, das Bundesamt für Verfassungsschutz oder Landesämter für Verfassungsschutz den Einsatz von Pegasus für eigene Zwecke geprüft haben oder einsetzen?*

Zu 4.:

Mit Blick auf die Abgrenzung der Verantwortungsbereiche im föderalen System der Bundesrepublik Deutschland nimmt die Landesregierung grundsätzlich keine Stellung zu Vorgängen in Behörden des Bundes oder anderer Länder.

5. *inwiefern und unter welchen Umständen sie einen Einsatz von „Pegasus“ sowie anderer sogenannter Staatstrojaner durch deutsche oder baden-württembergische Nachrichtendienste und Strafverfolgungsbehörden als sinnvoll erachten würde und wie sie dies verfassungsrechtlich bewertet?*

6. *inwiefern sie eine Änderung der Rechtslage, um den Einsatz von „Pegasus“ zu ermöglichen, für notwendig und sinnvoll erachtet?*

Zu 5. und 6.:

Die Übertragung von Telekommunikationsinhalten erfolgt aufgrund der zunehmenden Nutzung von Internettelefonie und internetbasierten Messengerdiensten zwischenzeitlich überwiegend in verschlüsselter Form. Für die Sicherheitsbehörden ergibt sich hierdurch ein zunehmender Erkenntnisverlust bei der klassischen Telekommunikationsüberwachung (Problem des „going dark“), wodurch insbesondere die Abwehr von Gefahren sowie die Verfolgung von Straftaten erheblich erschwert wird. Mit Blick auf die technische Komplexität können die Maßnahmen der Quellen-Telekommunikationsüberwachung oder Onlinedurchsuchung diesen Erkenntnisverlust – unabhängig vom Einsatz eines konkreten Produkts – zwar nicht ausgleichen, allerdings in besonders bedeutenden Einzelfällen zumindest punktuell Abhilfe schaffen.

Die Polizei Baden-Württemberg kann die Quellen-Telekommunikationsüberwachung sowohl zur Strafverfolgung nach der Strafprozessordnung (StPO) als auch zur Gefahrenabwehr nach dem Polizeigesetz Baden-Württemberg (PolG BW) anwenden. Das Instrument der Online-Durchsuchung steht der Polizei Baden-Württemberg hingegen lediglich zur Verfolgung von Straftaten (StPO), nicht jedoch zur Abwehr von Gefahren (PolG BW) zur Verfügung.

Das Landesamt für Verfassungsschutz Baden-Württemberg (LfV) hat unter den Voraussetzungen des § 5d des Gesetzes über den Verfassungsschutz in Baden-Württemberg (Landesverfassungsschutzgesetz) in Verbindung mit den Vorschriften des Artikel 10-Gesetzes die Möglichkeit, im Einzelfall mit technischen Mitteln verdeckt auf informationstechnische Systeme zuzugreifen, um laufende Telekommunikation zu überwachen.

Hinsichtlich der verfassungsrechtlichen Bewertung wird auf die Rechtsprechung des Bundesverfassungsgerichts (insbesondere das Urteil vom 27. Februar 2008 [1 BvR 370/07, 1 BvR 595/07], das Urteil vom 20. April 2016 [1 BvR 966/09, 1 BvR 1140/09] sowie den Beschluss vom 21. Juli 2021 [1 BvR 2771/18]), die Begründung zum Gesetz zur Änderung des Polizeigesetzes und des Gesetzes über die Ladenöffnung in Baden-Württemberg (LT-Drs. 16/2741), die Begründung zum Gesetz zur Änderung des Landesverfassungsschutzgesetzes und des Ausführungsgesetzes zum Artikel 10-Gesetz vom 28. November 2017 sowie die Stellungnahme des Ministeriums des Inneren, für Digitalisierung und Kommunen zum Antrag der Abg. Dr. Ulrich Goll u.a. FDP/DVP (LT-Drs. 16/2396) verwiesen.

Im Übrigen wird auf die Antwort zu Ziffer 3 verwiesen.

7. *ob ihr bekannt ist, ob „Pegasus“ auf Mobiltelefone von Regierungsmitgliedern des Landes Baden-Württemberg oder naher Familienmitglieder aufgespielt wurde und diese in Folge überwacht wurden?*

8. *ob ihr bekannt ist, ob „Pegasus“ auf Mobiltelefone von Mitglieder des Landtags, Bundestags und Europaparlaments oder ihrer Mitarbeiter aufgespielt wurde und diese in Folge überwacht wurden?*

9. *ob ihr bekannt ist, ob in Baden-Württemberg tätige Journalisten durch den Einsatz von „Pegasus“ überwacht wurden?*

10. *ob ihr sonstige Fälle des Einsatzes der „Pegasus“-Software und davon Betroffenen in Baden-Württemberg bekannt sind?*

Zu 7. bis 10.:

Es sind bislang keine Fälle einer entsprechenden Betroffenheit der in den Ziffern 7 bis 10 genannten Personenkreise bekannt.

11. *welche Maßnahmen sie trifft, damit die von Regierungsmitgliedern und ihren Familien genutzten Mobiltelefone nicht durch „Pegasus“ bzw. vergleichbare Spyware überwacht werden können?*

12. *ob sie diese Mobiltelefone aus welchen Gründen konkret auf Spuren der „Pegasus“-Software untersucht hat bzw. darauf verzichtet?*

Zu 11. und 12.:

Die Absicherung der dienstlichen Mobiltelefone von Regierungsmitgliedern erfolgt im Rahmen des Mobile Device Managements nach dem Stand der Technik durch die BITBW. Aufgrund der Art der für Spyware wie „Pegasus“ genutzten Angriffsvektoren, der anzunehmenden Professionalität des oder der Angreifer sowie der mutmaßlichen Leistungsfähigkeit bzw. des Funktionsumfangs der Software gestaltet sich eine zielführende, generelle und proaktive Umsetzung präventiver Schutzmaßnahmen allerdings äußerst schwierig. Eine potenzielle Kompromittierung der abgesicherten Geräte kann nicht in jedem Fall ausgeschlossen werden. Unmittelbar nach Bekanntwerden der Pegasus-Problematik hat das Ministerium des Inneren, für Digitalisierung und Kommunen damit begonnen, die Umsetzung eines zeitnahen „Vor-Ort-Prüfangebots“

zur Überprüfung von iOS-Geräten vorzubereiten. Dieses Angebot richtet sich zunächst an die Ressortspitzen und die Leitung der Regierungspräsidien. Eine Ausweitung des Adressatenkreises ist aufgrund der dann gemachten Erfahrungen zu prüfen. Das Konzept des Prüfangebots wird derzeit mit den zuständigen Spezialisten entwickelt. Mit der Überprüfung selbst soll Anfang September begonnen werden. An der Vorgehensweise Baden-Württembergs orientieren sich auch andere Länder.

Am Ende der Kalenderwoche 30 stand die beim Landeskriminalamt Baden-Württemberg (LKA BW) angegliederte Zentrale Ansprechstelle Cybercrime mit dem Informationssicherheitsbeauftragten des Landtags von Baden-Württemberg in Kontakt und wies auf die bereits unter Ziffer 2 erwähnte Warnmeldung des BSI, die darin enthaltene Bewertung sowie auf Präventionsmöglichkeiten hin. Zudem wurde das Angebot unterbreitet, dass sich Betroffene bei dem Feststellen von Indizien für eine Infiltrierung ihres Smartphones an das LKA BW wenden können.

Darüber hinaus steht die im Jahr 2019 beim LKA BW eingerichtete Zentrale Ansprechstelle für Amts- und Mandatsträger bereit, eine landesweit einheitliche, sachgerechte und zeitnahe Bearbeitung entsprechender Sachverhalte sowie eine grundsätzliche und anlassbezogene Sensibilisierung und Beratung von Amts- und Mandatsträgern zu gewährleisten. Sofern anlassbezogen Bedarf besteht, kann im Rahmen der Beratung und der gegebenenfalls weiteren Maßnahmen auch auf den Warnhinweis des BSI und die darin dargestellten Präventionsmöglichkeiten eingegangen werden.

Im konkreten Fall einer Betroffenheit, aber auch darüber hinaus, steht zudem das LfV als Ansprechpartner zur Verfügung und kann ggf. konkrete wie grundsätzliche präventive Handlungsempfehlungen geben.

13. *ob ihr gezielte Angriffsversuche auf Regierungsmitglieder oder andere hochrangige Politiker in Baden-Württemberg allgemein durch Spyware bekannt sind und welche Folgen diese jeweils nach sich gezogen haben?*

14. *ob ihr sonstige Fälle von Angriffen mittels Spyware in Baden-Württemberg bekannt sind und welche Folgen diese jeweils nach sich gezogen haben?*

Zu 13. und 14.:

Das Interesse fremder Nachrichtendienste an den klassischen Aufklärungsfeldern Politik, Militär, Wirtschaft, Wissenschaft und Verwaltung ist in Baden-Württemberg anhaltend hoch. In diesen Zusammenhängen hat das LfV in der Vergangenheit zahlreiche nachrichtendienstlich gesteuerte Angriffe beobachtet und bearbeitet, bei denen zum Teil auch Spyware eingesetzt wurde, und gegenüber dem geheim tagenden Parlamentarischen Kontrollgremium des Landtags dazu berichtet. Hinsichtlich der Lage in Baden-Württemberg wird auf die Ausführungen auf S. 306 ff. des Verfassungsschutzberichts 2020 verwiesen.

Zu mittels Spyware begangenen Straftaten können keine belastbaren Aussagen getroffen werden. Die Fallerfassung erfolgt nach den bundeseinheitlichen „Richtlinien für die Führung der Polizeilichen Kriminalstatistik“. Zwar werden in diesem Rahmen Delikte des Ausspähens und Abfangens von Daten erfasst, jedoch lassen sich diese nicht weiter nach dem jeweils eingesetzten Tatmittel aufschlüsseln.

Mit freundlichen Grüßen
in Vertretung des Ministers

gez. Julian Würtenberger
Staatssekretär