Deutscher Bundestag **Drucksache 20/131**

20. Wahlperiode 25.11.2021

Kleine Anfrage

der Abgeordneten Martina Renner, Nicole Gohlke, Sevim Dağdelen, Anke Domscheit-Berg, Dr. André Hahn, Andrej Hunko, Ina Latendorf, Ralph Lenkert, Petra Pau, Victor Perli, Dr. Petra Sitte, Kathrin Vogler und der Fraktion DIE LINKE.

Einsatz von Produkten zur informationstechnischen Überwachung der Firma „Candiru Limited“ durch deutsche Sicherheitsbehörden

Im Juli dieses Jahres war bekannt geworden, dass weltweit Journalisten, Menschenrechtsaktivistinnen und Menschenrechtsaktivisten, Geschäftsleute und Regierungspolitiker Opfer von Überwachungsmaßnahmen mithilfe des Programms „Pegasus“ der u. a. in Israel beheimateten Firma „NSO Group Technologies“ geworden waren (vgl. Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE. „Einsatz der Spionagesoftware „Pegasus“ in Deutschland“ auf Bundestagsdrucksache 19/32246, Vorbemerkung der Fragesteller). Inzwischen wurde öffentlich, dass sowohl das Bundeskriminalamt (BKA) als auch der Bundesnachrichtendienst (BND) die Software der NSO Group einsetzen (tagesschau.de vom 7. September 2021, „BKA soll Seehofer nicht informiert haben“; ZEIT online vom 8. Oktober 2021, „Bundesnachrichtendienst setzt umstrittene Cyberwaffe ein“).

Die US-Regierung gab am 3. November 2021 bekannt, dass die NSO Group, deren Produkte durch Bundesbehörden eingesetzt werden, auf die US-Sanktionsliste gesetzt wurde. Denn der Einsatz von „Pegasus“ habe sich u. a. gegen befreundete Politiker und Regierungen, Journalisten und Menschenrechtsaktivisten und damit gegen die Interessen der USA gerichtet (https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list; https://www.sueddeutsche.de/wirtschaft/nso-pegasus-spaehsoftware-usa-1.5455882). Neben der NSO Group wurde auch die israelische Softwarefirma „Candiru Limited“ (seit 2020 „Saito Tech Limited“) wegen derselben Vorwürfe auf die Sanktionsliste gesetzt. Die von jener Firma entwickelte und vertriebene Spyware soll sich insbesondere gegen Desktopanwendungen und Computer mit Windows-Betriebssystem richten. Verschiedene IT-Sicherheitsforscher des „Citizen Lab“ der Universität Toronto/Kanada, aber auch von Microsoft selbst haben inzwischen den Einsatz der Spionagesoftware gegen mindestens 100 betroffene Politiker, Journalisten, Menschenrechtsaktivisten oder Dissidenten aufgedeckt, auch in Westeuropa (https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/; https://netzpolitik.org/2021/penisfisch-bundesregierung-verweigert-auskunft-ueber-israelischen-staatstrojaner-candiru/). Die Software von Candiru wird also offenkundig in einem vergleichbaren, mindestens den Interessen der US-Regierung widersprechenden Rahmen eingesetzt.

Die Bundesregierung hat zuletzt die Auskunft darüber verweigert, ob Bundesbehörden Lizenzen der Spyware von „Candiru Limited“ (seit 2020 „Saito Tech

Limited“) erworben haben bzw. Leistungen dieser Firma nutzen (Bundestagsdrucksache 19/32490, Antwort auf die Schriftliche Frage 39). Angesichts der Entscheidung der US-Regierung erscheint trotz berührter Staatswohlbelange eine öffentliche Positionierung der Bundesregierung erforderlich. Denn die Zusammenarbeit mit den von US-Sanktionen betroffenen Unternehmen und der Einsatz ihrer Produkte durch Behörden des Bundes wird nach Ansicht der Fragestellerinnen und Fragesteller die Zusammenarbeit und Beziehungen zu US-amerikanischen Behörden und Diensten belasten und seinerseits Belange des Staatswohls nachhaltig beschädigen. Angesichts dessen scheint aus Sicht der Fragestellerinnen und Fragesteller eine weitere Verweigerung entsprechender Auskünfte aufgrund des überragenden öffentlichen und parlamentarischen Interesses ausgeschlossen.

Wir fragen die Bundesregierung:

1. Haben Vertreter oder Beauftragte des Unternehmens „Candiru Limited“ (seit 2020 „Saito Tech Limited“) Behörden des Bundes bzw. den Vertretern von Behörden die von ihnen entwickelten und vertriebenen Softwareprodukte zur Infiltration und Überwachung informationstechnischer Systeme und Netzwerke vorgestellt, und wenn ja, wann, und welchen Behörden?
2. Waren Produkte und Leistungen zur informationstechnischen Überwachung im Angebot des Unternehmens „Candiru Limited“ (seit 2020 „Saito Tech Limited“) Gegenstand der Marktsichtung durch die Zentralstelle für Informationstechnik im Sicherheitsbereich (ZITiS) oder Bedarfsträger im Geschäftsbereich der Bundesregierung?
3. Hat sich ZITiS insbesondere hinsichtlich des verfassungskonformen Einsatzes mit Produkten und Leistungen im Angebot des Unternehmens „Candiru Limited“ (seit 2020 „Saito Tech Limited“) zur informationstechnischen Überwachung beschäftigt, und wenn ja, wann, und mit welchem Ergebnis?
4. Wer wurde von ZITiS gegebenenfalls wann über das Ergebnis dieser Prüfung unterrichtet, und wie hat die zuständige Fach- und Rechtsaufsicht sich zu diesem Prüfergebnis verhalten?
5. Inwieweit wurde ZITis gegebenenfalls vom Einsatz, einschließlich Test- oder Erprobungseinsatz von Produkten und Leistungen im Angebot des Unternehmens „Candiru Limited“ (seit 2020 „Saito Tech Limited“) zur informationstechnischen Überwachung in Kenntnis gesetzt oder hat Kenntnis von technischen Fragen und Problemstellungen im Rahmen des Einsatzes (etwa zum Aufbau von Know-how für zukünftige Beschaffungen in diesem Bereich) erhalten?
6. Hat die Bundesregierung alle gegebenenfalls infrage kommenden Gremien des Deutschen Bundestages für den Fall eines Ankaufs und eines Einsatzes von Produkten und Leistungen zur informationstechnischen Überwachung im Angebot des Unternehmens „Candiru Limited“ (seit 2020 „Saito Tech Limited“) durch Behörden im Zuständigkeitsbereich dieser Gremien unterrichtet?

   Wenn nein, warum ist eine solche Unterrichtung bislang unterblieben?
7. Wurde gegebenenfalls eine technische Prüfung der Produkte und Leistungen zur informationstechnischen Überwachung im Angebot des Unternehmens „Candiru Limited“ (seit 2020 „Saito Tech Limited“) durch das Bundesamt für Sicherheit in der Informationstechnik durchgeführt, wenn ja, wann, und mit welchem Ergebnis, wenn nein, warum nicht?

8. Nach welchen Kriterien, Schemata, fachlichen Vorgaben oder Fragestellungen wurde gegebenenfalls eine Überprüfung der Produkte und Leistungen zur informationstechnischen Überwachung im Angebot des Unternehmens „Candiru Limited“ (seit 2020 „Saito Tech Limited“) durch die einsetzenden Behörden selbst vorgenommen?
9. Hat jede einsetzende Behörde gegebenenfalls selbst eine solche Überprüfung vorgenommen, und wussten die jeweiligen Behörden von der Beschaffung und dem Einsatz in den anderen Behörden des Bundes?
10. Welche Behörden oder Einrichtungen wurden gegebenenfalls anlässlich bzw. im Nachgang eigener Überprüfungen der einsetzenden Behörden über die Ergebnisse dieser Überprüfungen unterrichtet?
11. Waren die geschäftsführenden Bundesministerien gegebenenfalls anlässlich bzw. im Nachgang über den Einsatz und über die Ergebnisse von Überprüfungen der Produkte und Leistungen zur informationstechnischen Überwachung im Angebot des Unternehmens „Candiru Limited“ (seit 2020 „Saito Tech Limited“) informiert, und wenn ja, wer wurde jeweils wann und worüber unterrichtet?
12. Hat sich nach Kenntnis der Bundesregierung infolge von möglichen Überprüfungen bzw. Auswertungen des Einsatzes ergeben, dass die den Behörden des Bundes zur Verfügung gestellten Programmversionen von Produkten und Leistungen zur informationstechnischen Überwachung im Angebot des Unternehmens „Candiru Limited“ (seit 2020 „Saito Tech Limited“) weiterer Einschränkungen bedürfen, und wenn ja, seit wann ist das bekannt geworden, und wann wurde dies entsprechend umgesetzt?
13. Wurden den zuständigen Kontrollgremien bzw. Gerichten Informationen über Produkte und Leistungen zur informationstechnischen Überwachung im Angebot des Unternehmens „Candiru Limited“ (seit 2020 „Saito Tech Limited“) zu Verfügung gestellt, die den Einsatz im Rahmen von Gefahrenabwehrvorgängen oder Strafermittlungen bzw. als nachrichtendienstliches Mittel genehmigt bzw. angeordnet haben, und wenn ja, welche?
14. Wurden Produkte und Leistungen zur informationstechnischen Überwachung im Angebot des Unternehmens „Candiru Limited“ (seit 2020 „Saito Tech Limited“) bislang eingesetzt, und wenn ja, in wie vielen Fällen mit wie vielen Betroffenen, und
    a) wie viele dieser Vorgänge sind noch laufend,
    b) wie viele dieser Vorgänge sind bereits abgeschlossen,
    c) welches Ziel wurde mit dem jeweiligen Einsatz verfolgt (Fernmeldeaufklärung, nachrichtendienstliches Mittel, Gefahrenabwehr, Strafverfolgung)?
15. In wie vielen Fällen erfolgte – sofern Frage 14 bejaht wird – bislang nach Abschluss der Maßnahme eine Information an Betroffene, in wie vielen Fällen wurde vorläufig von einer Benachrichtigung abgesehen oder soll dauerhaft davon abgesehen werden?
16. Welchen Schweregrad (base score) nach dem Common Vulnerability Scoring System (CVSS) haben – sofern Frage 14 bejaht wird – die beim Einsatz der Produkte von Candiru/Saito genutzten Vektoren zur Ausleitung von Daten aus dem jeweiligen Zielsystem?

17. Welche Kosten sind gegebenenfalls jeweils durch die Beschaffung, den Betrieb und die Wartung von Produkten der „Candiru Ltd.“ bzw. „Saito Tech Ltd.“ für Behörden des Bundes bislang entstanden (bitte nach Behörde und Jahr aufschlüsseln)?

Berlin, den 15. November 2021

Amira Mohamed Ali, Dr. Dietmar Bartsch und Fraktion

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333