Deutscher Bundestag **Drucksache 20/3840**

20. Wahlperiode 05.10.2022

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Martina Renner, Nicole Gohlke, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 20/3544 –

Maßnahmen zur Stärkung der Cybersicherheit versus Einsatz von Produkten zur informationstechnischen Überwachung

Vorbemerkung der Fragesteller

Nachdem in den vergangenen Monaten der extensive Einsatz von Spähsoftware der israelischen Softwarefirma NSO Group welt- und europaweit für Schlagzeilen gesorgt hat, findet inzwischen eine breit angelegte Untersuchung hierzu durch das EU-Parlament statt (u. a. https://netzpolitik.org/2022/untersuchungsausschuss-staatstrojaner-pegasus-wird-alle-40-minuten-eingesetzt/). Nach Angaben des israelischen Herstellers wird das zum Ausspähen bzw. zur Komplettübernahme von Mobiltelefonen nutzbare Programm in weltweit ca. 50 Ländern eingesetzt. Zu den Zielen der das Programm einsetzenden Behörden gehörten u. a. Oppositionspolitiker in Polen und Spanien oder Journalisten in Ungarn, Marokko oder Chile (https://netzpolitik.org/2021/staatstrojaner-polnische-oppositionelle-mit-pegasus-gehackt/; https://netzpolitik.org/2022/nso-group-zwoelf-eu-laender-nutzen-pegasus-staatstrojaner/; https://www.zeit.de/politik/ausland/2021-11/ungarn-pegasus-spionagesoftware-nso-group-fidesz-regierung-nutzung). Während die offiziellen Untersuchungen also noch anhalten, sind andere Schwachstellen und Sicherheitslücken lange bekannt, aber es ist unklar, ob und inwiefern deutsche und europäische Behörden insoweit überhaupt tätig werden.

So berichtete „DER SPIEGEL“, dass die italienische Firma Tykelab beispielsweise Überwachungsangriffe anböte, wobei u. a. eine lange bekannte Sicherheitslücke im SS7-Protokoll der Mobilfunkanbieter und Mobilfunkunternehmen zu Überwachungszwecken ausgenutzt würde (https://www.spiegel.de/netzwelt/web/ss7-angriffe-von-tykelab-wie-eine-italienische-firma-das-globale-telefonnetz-attackiert-a-087b4f50-f167-4b6e-a6ac-fddd40626974). Diese Sicherheitslücke ist auch nach Aussagen der Bundesregierung bekannt. Das Bundesamt für die Sicherheit in der Informationstechnik (BSI) arbeite gemeinsam mit anderen Stellen bereits seit längerem an der Beseitigung dieser Sicherheitslücke auf der Ebene der Global System for Mobile Communications Association (GSMA) und stehe auch im Austausch mit den deutschen Netzbetreibern (Antwort auf die Schriftliche Frage 61 auf Bundestagsdrucksache 19/18555). Allerdings scheint sich die Bundesregierung über die Tragweite dieser Sicherheitslücke im Unklaren zu sein und auf geeignete Maßnah-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern und für Heimat vom 5. Oktober 2022 übermittelt.
Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

men der in Deutschland tätigen Mobilfunkbetreiber zu verlassen (Antwort auf die Mündliche Frage 7, Plenarprotokoll 19/155).

Das Online-Medium „euobserver“ berichtete, dass die italienischen Softwareunternehmen Tykelab und RCS Lab SpA, die zur Unternehmensgruppe Cy4gate gehören, nicht nur verschiedene Hacking-Tools innerhalb und außerhalb der EU anböten und einsetzen und dabei u. a. durch Untersuchungen seitens Googles Threat Analysis Group enttarnt worden sei (https://euobserver.com/digital/155849; https://indianexpress.com/article/technology/tech-news-technology/rcs-lab-hack-how-android-ios-users-in-italy-and-kazakhstan-were-spied-on-7988039/). Die Firma RCS Lab bietet ihre Überwachungssoftware „Ubique“ mit dem Versprechen an, „die Bewegung von fast jedem, der ein Mobiltelefon bei sich trägt, zu verfolgen“. Die teils mit „Pegasus“ verglichene Überwachungssoftware „Hermit“ ermöglicht eine komplette Übernahme der Zielgeräte inklusive Ferneinschaltung des Mikrofones (https://posteo.de/news/italienische-spionagefirmen-erm%C3%B6glichen-umfassende-handy-%C3%BCberwachung). Der Einsatz dieser Software wurde u. a. aus Kasachstan, Italien und Rumänien berichtet. Googles Sicherheitsforscher haben auch herausgefunden, dass RCS Lab auch mit der hochumstrittenen Spähsoftware-Firma Hacking Team zusammen gearbeitet hatte (https://www.heise.de/news/Google-Android-und-Apple-Handys-von-italienischer-Spyware-ausgespaeht-7151984.html). Mitglieder des Pegasus-Untersuchungsausschusses des EU-Parlaments haben bereits erklärt, sich auch mit diesen Überwachungstools beschäftigen zu wollen.

Vorbemerkung der Bundesregierung

Die Bundesregierung beantwortet die im Rahmen des parlamentarischen Fragerechts angefragten Sachverhalte gegenüber dem Deutschen Bundestag grundsätzlich öffentlich, transparent und vollständig, um dem verfassungsrechtlich verbrieften Aufklärungs- und Informationsanspruch des Deutschen Bundestages zu entsprechen. Soweit erfragte Informationen Umstände betreffen, die aus Gründen des Staatswohls geheimhaltungsbedürftig sind, hat die Bundesregierung zu prüfen, ob und auf welche Weise die Geheimhaltungsbedürftigkeit mit dem parlamentarischen Informationsanspruch in Einklang gebracht werden kann, und gegebenenfalls alternative Formen der Informationsvermittlung zu suchen, die das Informationsinteresse des Parlaments unter Wahrung der berechtigen Geheimhaltungsinteressen der Regierung befriedigen (BVerfGE 124, S. 161,193).

Nach sorgfältiger Abwägung des Aufklärungs- und Informationsrechts der Abgeordneten mit dem Wohl des Bundes (Staatswohl), das durch Bekanntwerden geheimhaltungsbedürftiger Informationen gefährdet werden könnte, äußert sich die Bundesregierung nicht, weil dies die Wirksamkeit sicherheitsbehördlicher Tätigkeit gefährden kann. Evident geheimhaltungsbedürftige Informationen muss die Bundesregierung nach der Rechtsprechung des Bundesverfassungsgerichts nicht offenlegen (BVerfGE 124, 161, 193 f.).

Soweit die Fragen nicht explizit an das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) gerichtet sind, geht die Bunderegierung im Kontext der Fragestellung davon aus, dass sich die Fragen auf die Strafverfolgungs-, Ermittlungs- und Gefahrenabwehrbehörden des Bundes sowie der Nachrichtendienste des Bundes beziehen. Dementsprechend werden ausschließlich diese in die Beantwortung einbezogen.

Die Bundesregierung ist nach sorgfältiger Prüfung zu der Auffassung gelangt, dass aufgrund der Schutzbedürftigkeit der erfragten Informationen bezüglich der Strafverfolgungs-, Ermittlungs- und Gefahrenabwehrbehörden des Bundes sowie der Nachrichtendienste des Bundes aufgrund entgegenstehender über-

wiegender Belange des Staatswohls nicht bzw. teilweise nicht erfolgen kann, auch nicht in eingestufter Form.

Im Einzelnen:

Die Antwort zu Frage 16 ist in Teilen als „VS – Nur für den Dienstgebrauch“ eingestuft. Die erbetenen Auskünfte sind in Teilen geheimhaltungsbedürftig, weil sie Informationen enthalten, die im Zusammenhang mit der Arbeitsweise und Methodik der von der Kleinen Anfrage betroffenen Behörden des Bundes und insbesondere deren Aufklärungsaktivitäten und Analysemethoden stehen. Die Fragen betreffen zum Teil detaillierte Einzelheiten zu ihren technischen Fähigkeiten und ermittlungstaktischen Verfahrensweisen. Aus dem Bekanntwerden der Antworten könnten Rückschlüsse auf Vorgehensweise, Fähigkeiten und Methoden der Sicherheitsbehörden gezogen werden, was wiederum nachteilig für die Aufgabenerfüllung der durchführenden Stellen und damit für die Interessen der Bundesrepublik Deutschland sein kann.

Deshalb ist die Antwort zur genannten Frage 16 gemäß § 2 Absatz 2 Nummer 4 der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz (VS-Anweisung – VSA) in Teilen als „VS – Nur für den Dienstgebrauch“ eingestuft und wird als nicht zur Veröffentlichung in einer Bundestagsdrucksache bestimmte Anlage übermittelt.

Nach sorgfältiger Abwägung ist die Bundesregierung zu der Auffassung gelangt, dass eine Beantwortung der Fragen 7 bis 13, 15 und 16 bezüglich der Strafverfolgungs-, Ermittlungs- und Gefahrenabwehrbehörden des Bundes sowie der Nachrichtendienste des Bundes aufgrund entgegenstehender überwiegender Belange des Staatswohls teilweise nicht oder nicht erfolgen kann, auch nicht in eingestufter Form.

Die insoweit erbetenen Informationen zielen auf die kriminaltaktischen oder nachrichtendienstlichen Ermittlungs- bzw. Informationsgewinnungsinstrumente der betroffenen Sicherheitsbehörden ab. Mit der Beantwortung würden mittelbar bestimmte Arbeitsmethoden und Vorgehensweisen im Bereich der technischen Aufklärung offengelegt oder Rückschlüsse darauf ermöglicht. Hierdurch würden die Arbeitsfähigkeit und Aufgabenerfüllung und somit die Erfüllung des gesetzlichen Auftrags der betroffenen Sicherheits- und Strafverfolgungsbehörden sowie Nachrichtendienste erheblich gefährdet.

Eine VS-Einstufung und Hinterlegung der angefragten Informationen in der Geheimschutzstelle des Deutschen Bundestages kommt angesichts ihrer erheblichen Brisanz im Hinblick auf die Bedeutung der technischen Aufklärung für die Aufgabenerfüllung der Sicherheitsbehörden des Bundes nicht in Betracht. Das Risiko, dass derart sensible Informationen bekannt werden, kann unter keinen Umständen hingenommen werden. Die angefragten Informationen beschreiben die technischen Fähigkeiten der betroffenen Sicherheitsbehörden bzw. Nachrichtendienste des Bundes aufgrund ihres Bezuges auf bestimmte Produkte bzw. Hersteller in einem derartigen Detaillierungsgrad, dass eine Bekanntgabe auch gegenüber einem begrenzten Kreis von Empfängern ihrem Schutzbedürfnis nicht Rechnung tragen würde.

Die einzelnen Kooperationspartner arbeiten mit Sicherheits- und Strafverfolgungsbehörden sowie Nachrichtendiensten nur unter der Voraussetzung zusammen, dass die konkrete Kooperation mit ihnen – auch nicht mittelbar – preisgegeben, sondern absolut vertraulich behandelt wird. Dies bedeutet, dass die geheimhaltungsbedürftigen Informationen zu und aus der Kooperation nicht außerhalb der Sicherheits- und Strafverfolgungsbehörden sowie Nachrichtendienste weitergegeben werden dürfen. Eine Offenlegung der Kooperationspartner würde das Ansehen von deutschen Nachrichtendiensten und das Vertrauen in diese daher weltweit erheblich schädigen. Dementsprechend bestünde die

ernstzunehmende Gefahr eines weitreichenden Wegfalls von Kooperationsmöglichkeiten nicht nur bei zivilen Firmen. Würde die Bundesregierung die Informationen freigeben, so wäre zudem zu befürchten, dass Kooperationspartner ihrerseits die Vertraulichkeit nicht oder nur noch eingeschränkt wahren würden.

In der Konsequenz könnte es künftig zu einem Rückgang oder zum Wegfall zukünftiger Vertragspartner und in der Folge zu einem Wegfall der Erkenntnisgewinnung der deutschen Nachrichtendienste kommen. Dies alles würde dem deutschen Staatswohl zuwiderlaufen. Dies hätte signifikante Informationslücken und negative Folgewirkungen für die Abbildung der Sicherheitslage in der Bundesrepublik Deutschland sowie im Hinblick auf den Schutz deutscher Interessen im Ausland zur Folge. Insofern muss ausnahmsweise das Fragerecht der Abgeordneten gegenüber dem Geheimhaltungsinteresse der Bundesregierung zurückstehen.

1. Besteht die beschriebene Sicherheitslücke im Signalisierungssystem SS7, welche durch „Tykelab“ ausgenutzt worden sein soll, nach Kenntnis der Bundesregierung bei Mobilfunkunternehmen fort, die ihre Dienste in Deutschland bzw. der EU anbieten?

2. Wenn ja, welche Unternehmen (Mobilfunkunternehmen, Netzbetreiber) sind davon betroffen?

Die Fragen 1 und 2 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Belastbare Informationen darüber, ob die beschriebene Sicherheitslücke von den Mobilfunkanbietern, die ihre Dienste in Deutschland und in der EU anbieten, inkl. Mobile virtual network operators (MVNOs), fortbesteht, liegen der Bundesregierung nicht vor.

3. Sind der Bundesregierung Maßnahmen dergestalt bekannt, dass die betreffenden Mobilfunkunternehmen ihre Kunden über die bestehenden Risiken aufklären und informieren, beispielsweise anlässlich von Hacking-Angriffen gegen Netzbetreiber oder ähnlicher Vorfälle?

Die Bundesnetzagentur (BNetzA) hat vor mehreren Monaten angeordnet, dass eine kostenlose Sprachnachricht abgespielt werden muss, bevor ein teures Telefonat in bestimmte Länder zustande kommt. Dies war eine Gegenmaßnahme zu „Wangiri-Fraud“, also einer Missbrauchsform, die den Teilnehmer animiert, eine teure Nummer zu wählen, weil er von dieser einen verpassten Anruf bekommen hat.

Darüber hinaus liegen der Bundesregierung keine Erkenntnisse vor, in dem Informationen über SS7- oder andere Signalisierungsangriffe, die in erster Linie eine Schwachstelle in der Infrastruktur des Betreibers betreffen, als allgemeine Information (präventiv) an die Teilnehmer weitergegeben wurden.

4. Welche Maßnahmen wurden wann seitens des BSI gegenüber in Deutschland tätigen Mobilfunkunternehmen im Zusammenhang mit der Beseitigung dieser Schwachstelle ergriffen bzw. vorangetrieben?

5. Welche Maßnahmen wurden wann seitens des BSI gemeinsam mit anderen Partnern auf der Ebene der Global System for Mobile Communications Association zur Beseitigung dieser Schwachstelle ergriffen bzw. vorangetrieben?

Die Fragen 4 und 5 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Das BSI beteiligt sich an den laufenden Aktivitäten zu den Signalisierungsprotokollen für das 5G-Roaming, welche langfristig das SS7-Protokoll ablösen werden. Allerdings wird das schwachstellenbehaftete SS7-Protokoll auf absehbare Zeit weiter unterstützt werden. Bekannte Angriffe können mit speziellen SS7-Firewalls erkannt und abgewehrt werden. Hierzu befindet sich das BSI mit Unternehmen im Austausch.

6. Welche Haltung nimmt die Bundesregierung bzw. das BSI bei den Beratungen auf der Ebene der Global System for Mobile Communications Association in diesem Zusammenhang ein?

Das BSI setzt sich setzt sich im Rahmen seiner Zuständigkeit dafür ein, dass die Roaming-Signalisierung Ende-zu-Ende, d. h. zwischen den beiden Roaming-Partnern (MNOs) kryptographisch gesichert wird, so dass Vermittlerinstanzen, die ebenfalls Zugriff auf den Signalisierungsverkehr haben, diesen nicht unerkannt manipulieren können.

7. Haben Vertreter oder Beauftragte des Unternehmens Tykelab welchen Behörden des Bundes bzw. den Vertretern welcher Behörden die von ihnen entwickelten und vertriebenen Softwareprodukte zur Infiltration und Überwachung informationstechnischer Systeme und Netzwerke vorgestellt, und wenn ja, wann?

8. Waren Produkte und Leistungen zur informationstechnischen Überwachung im Angebot des Unternehmens Tykelab Gegenstand der Marktsichtung durch die Zentralstelle für Informationstechnik im Sicherheitsbereich (ZITiS) oder Bedarfsträger im Geschäftsbereich der Bundesregierung?

Die Fragen 7 und 8 werden gemeinsam beantwortet.

Auf die Vorbemerkung der Bundesregierung wird verwiesen.

9. Wann und mit welchem Ergebnis hat sich ZITiS insbesondere hinsichtlich des verfassungskonformen Einsatzes mit Produkten und Leistungen im Angebot des Unternehmens Tykelab zur informationstechnischen Überwachung beschäftigt?

Die Befassung mit rechtlichen Fragen des verfassungskonformen Einsatzes von Produkten und Leistungen im Bereich der informationstechnischen Überwachung (ITÜ) obliegt den Behörden, die die ITÜ-Maßnahmen im Rahmen ihrer gesetzlichen Befugnisse durchführen.

Darüber hinaus wird auf die Vorbemerkung der Bundesregierung verwiesen.

10. Welchen Schweregrad (base score) nach dem Common Vulnerability Scoring System (CVSS) haben die beim Einsatz der Produkte von „Tykelab“ genutzten Vektoren zur Ausleitung von Daten aus dem jeweiligen Zielsystem?

11. Welche Kosten sind jeweils durch die Beschaffung, den Betrieb und die Wartung von Produkten der „Tykelab“ für Behörden des Bundes bislang entstanden bzw. werden künftig entstehen (bitte nach Behörde und Jahr aufschlüsseln)?

Die Fragen 10 und 11 werden gemeinsam beantwortet.

Auf die Vorbemerkung der Bundesregierung wird verwiesen.

12. Haben Vertreter oder Beauftragte des Unternehmens RCS Lab SpA welchen Behörden des Bundes bzw. den Vertretern welcher Behörden die von ihnen entwickelten und vertriebenen Softwareprodukte zur Infiltration und Überwachung informationstechnischer Systeme und Netzwerke vorgestellt, und wenn ja, wann?

13. Waren Produkte und Leistungen zur informationstechnischen Überwachung im Angebot des Unternehmens RCS Lab SpA Gegenstand der Marktsichtung durch die Zentralstelle für Informationstechnik im Sicherheitsbereich oder Bedarfsträger im Geschäftsbereich der Bundesregierung?

Die Fragen 12 und 13 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Zur Wahrnehmung ihrer Aufgaben hinsichtlich der Weiterentwicklung von Cyberfähigkeiten im Bereich der Informationstechnischen Überwachung steht die ZITiS seit 2019 mit Vertretern des Unternehmens „RCS Lab SpA“ in Kontakt, um im Rahmen einer Marktsichtung Informationen über das Portfolio des Unternehmens zu erhalten. Hierbei fanden zwei Termine im Jahr 2019, ein Termin im Jahr 2020 und zwei Termine im Jahr 2022 statt. Darüber hinaus wird auf die Vorbemerkung der Bundesregierung verwiesen.

14. Wann und mit welchem Ergebnis hat sich ZITiS insbesondere hinsichtlich des verfassungskonformen Einsatzes mit Produkten und Leistungen im Angebot des Unternehmens RCS Lab SpA zur informationstechnischen Überwachung beschäftigt?

Im Rahmen der Marktsichtung durch ZITiS wird die grundsätzliche Vereinbarkeit der gesichteten Technologien mit dem deutschen Rechtsrahmen mitbetrachtet.

Im Übrigen wird auf die Antwort zu Frage 9 verwiesen.

15. Welchen Schweregrad (base score) nach dem Common Vulnerability Scoring System haben die beim Einsatz der Produkte von „RCS Lab SpA“ genutzten Vektoren zur Ausleitung von Daten aus dem jeweiligen Zielsystem?

Auf die Vorbemerkung der Bundesregierung wird verwiesen.

16. Welche Kosten sind jeweils durch die Beschaffung, den Betrieb und die Wartung von Produkten der „RCS Lab SpA“ für Behörden des Bundes bislang entstanden bzw. werden künftig entstehen (bitte nach Behörde und Jahr aufschlüsseln)?

Es wird auf den als „VS – Nur für den Dienstgebrauch“* eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.

Darüber hinaus wird auf die Vorbemerkung der Bundesregierung verwiesen.

* Das Bundesministerium des Innern und für Heimat hat Teile der Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Teile der Antwort sind im Parlamentssekretariat des Deutschen Bundestages hinterlegt und können dort von Berechtigten eingesehen werden.

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.bundesanzeiger-verlag.de
ISSN 0722-8333