Deutscher Bundestag **Drucksache 19/32246**

19. Wahlperiode 01.09.2021

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Jan Korte, Sevim Dağdelen, Anke Domscheit-Berg, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 19/31809 –

Einsatz der Spionagesoftware „Pegasus“ in Deutschland

Vorbemerkung der Fragesteller

Nach Berichten eines internationalen Rechercheverbundes zahlreicher Medien, an dem aus Deutschland die „Süddeutsche Zeitung“, der „NDR“, „WDR“ und die Wochenzeitung „ZEIT“ beteiligt sind, sollen Regierungen weltweit „militärische Spionagesoftware“ der israelischen Firma NSO Group nicht nur für die Überwachung von Terroristen und Kriminellen nutzen, sondern auch für erfolgreiche Hacks von Smartphones, die Journalisten, Menschenrechtsaktivisten und Geschäftsleuten gehörten. Mit der Software, die als eine der leistungsfähigsten Spionageprogramme auf dem kommerziellen Markt gilt, kann „unbemerkt die komplette Kommunikation auf dem Mobiltelefon einer Zielperson überwacht werden kann – egal ob SMS, E-Mails oder verschlüsselte Chats. Auch Fotos und Videos können durchsucht und Passwörter ausgelesen werden. Und das alles sogar aus der Ferne, ohne physischen Zugriff auf das Telefon zu haben.“ (https://www.tagesschau.de/investigativ/ndr-wdr/spaeh-software-pegasus-deutschland-101.html). Die Smartphones können aber nicht nur heimlich überwacht und komplett ausgespäht werden, sondern sogar zu Wanzen umgewandelt werden, um unbemerkt Gespräche mitzuschneiden, wobei neben dem Mikrofon auch die Kamera eines Geräts unbemerkt eingeschaltet werden könne. Während auf der NSO-Website die Firma ihre Produkte als „Technologie, die Regierungsbehörden hilft, Terrorismus und Verbrechen zu verhindern und zu untersuchen“ anpreist, zeigen die Medienrecherchen, die sich auch auf Daten von Amnesty International stützen, dass mindestens 189 Journalistinnen und Journalisten, 85 Menschenrechtsaktivistinnen und Menschenrechtsaktivisten und mehr als 600 Politikerinnen und Politiker mit der Spionagesoftware weltweit ausgespäht wurden. Amnesty International hatte gemeinsam mit der Organisation Forbidden Stories einen Datensatz von mehr als 50 000 Telefonnummern ausgewertet, die als potenzielle Ausspähziele von Kunden der NSO Group ausgewählt worden seien. Unter den Ausgespähten finden sich auch investigative Journalisten aus Ungarn, Marokko oder Aserbaidschan sowie beispielsweise katalonische Unabhängigkeitsbefürworter in Spanien. Am 20. Juli 2021 berichtete u. a. „Spiegel Online“, dass unter den zahlreichen Ausgespähten auch etliche europäische Spitzenpolitiker, wie etwa der französische Präsident Emmanuel Macron und sein direktes Umfeld, „der damalige Premierminister Édouard Philippe sowie mehrere Ministerinnen und Minister in Frankreich ausgespäht werden, unter ihnen die noch amtierenden

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 1. September 2021 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

Kabinettsmitglieder Außenminister Jean-Yves Le Drian, Wirtschaftsminister Bruno Le Maire und Bildungsminister Jean-Michel Blanquer“ seien (https://www.spiegel.de/ausland/pegasus-emmanuel-macron-im-visier-der-cyberwaffe-a-28bfa163-4933-41af-8128-9d63ed5e2501). Besonders exzessiv ist die Software offenbar in Mexiko zum Einsatz gekommen, wo neben Journalisten u. a. auch das Umfeld des amtierenden Präsidenten ausgeforscht wurde (vgl. https://www.tagesschau.de/investigativ/ndr-wdr/spiongage-software-pegasus-mexiko-101.html). Laut forensischem Bericht von Amnesty International (https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/) zählten zur „Pegasus“-Infrastruktur auch 212 DNS-Server in Deutschland. Am 20. Juli 2021 berichtete RND, dass das Büro der Pariser Staatsanwaltschaft Ermittlungen zum mutmaßlich weit verbreiteten Einsatz der Spionagesoftware gegen Journalisten, Menschenrechtsaktivisten und Dissidenten in Frankreich aufgenommen habe und zu einer ganzen Reihe möglicher Anklagepunkte, darunter Verstoß gegen das Persönlichkeitsrecht, illegale Nutzung von Daten und illegaler Verkauf von Spionagesoftware, ermittelt werde.

In Deutschland ist die am 6. April 2017 errichtete Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) im Geschäftsbereich des Bundesministeriums des Innern, für Bau und Heimat damit betraut, Bundesbehörden mit Sicherheitsaufgaben im Hinblick auf informationstechnische Fähigkeiten zu unterstützen und zu beraten. Die ZITiS-IT-Fachleute entwickeln u. a. selbst Cyberwerkzeuge, mit denen Polizei und Verfassungsschutz verschlüsselte Kommunikation überwachen können, sichten aber auch den weltweiten Markt an Überwachungssoftware, deren Kauf sich für deutsche Sicherheitsbehörden lohnen könnte. Laut Bericht der „Tagesschau“ sollen NSO-Vertreter bei ZITiS 2018 in München vorstellig geworden sein: „Sie waren auf einer Art Roadshow und präsentierten ihr Portfolio“ (https://www.tagesschau.de/investigativ/ndr-wdr/spaeh-software-pegasus-deutschland-101.html), in dem sich auch die Spionagesoftware Pegasus befunden habe. „Ein Jahr zuvor, im Oktober 2017, wurde NSO schon beim Bundeskriminalamt (BKA) in Wiesbaden vorstellig. Ebenso gab es Gespräche mit dem BND und dem Bundesamt für Verfassungsschutz. Mit den Cyberexperten vom bayerischen Landeskriminalamt (LKA) trafen sich die Vertreter der israelischen Firma im Jahr 2019 sogar gleich zwei Mal. Bei einer weiteren Vorführung im September 2019 im Innenministerium in München war sogar Minister Joachim Herrmann anwesend, wie ein Sprecher mitteilte“ (ebd.). Bislang habe NSO in Deutschland aber „wohl nur Absagen“ erhalten, während es „an 60 unterschiedliche Behörden in 40 Ländern der Welt […] seine Produkte nach eigenen Angaben bereits verkauft“ hat (ebd.).

Am 21. Juli 2021 stellte das Bundesverfassungsgericht in seinem veröffentlichten Beschluss (1 BvR 2771/18; „IT-Sicherheitslücken“) klar, dass sich aus Artikel 10 des Grundgesetzes (GG) eine Schutzpflicht bezüglich bekannter Sicherheitslücken ergibt und „die grundrechtliche Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme verpflichtet den Staat, zum Schutz der Systeme vor Angriffen durch Dritte beizutragen“ (https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2021/06/rs20210608_1bvr277118.html).

Vorbemerkung der Bundesregierung

Zwar ist der parlamentarische Informationsanspruch grundsätzlich auf die Beantwortung gestellter Fragen in der Öffentlichkeit angelegt. Soweit parlamentarische Anfragen jedoch 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. Die Bundesregierung ist nach sorgfältiger Prüfung zu der Auffassung gelangt, dass aufgrund der Schutzbedürftigkeit der erfragten Informationen eine Beantwortung einzelner Fragen in offener Form nicht oder nur teilweise erfolgen kann.

Im Einzelnen:

Die Antworten zu den Fragen 14 und 15 sind als „VS – Nur für den Dienstgebrauch“ eingestuft. Die erbetenen Auskünfte sind 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 sind die Antworten zu den genannten Fragen 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 werden als nicht zur Veröffentlichung in einer Bundestagsdrucksache bestimmte Anlage übermittelt.

Die mit den Fragen 1, 2, 3, 4, 14 und 16 erbetenen Informationen berühren in weiten Teilen in besonders hohem Maße das Staatswohl. Nach sorgfältiger Abwägung ist die Bundesregierung zu dem Ergebnis gekommen, dass auch das geringfügige Risiko ihrer Offenlegung nicht getragen werden kann und deshalb die Fragen hinsichtlich der Sicherheitsbehörden des Bundes mit polizeilichen und nachrichtendienstlichen Aufgaben auch nicht in eingestufter Form beantwortet werden können.

Eine Bekanntgabe von Einzelheiten der bei diesen Behörden zur Bekämpfung von Kriminalität und Terrorismus im Rahmen ihrer jeweiligen Zuständigkeit eingesetzten Softwareprodukte für die Bearbeitung und Auswertung von Ermittlungsverfahren würde weitgehende Rückschlüsse auf die technischen Fähigkeiten sowie die taktischen Einzelheiten bzw. Arbeitsabläufe und damit mittelbar auch sowohl auf die derzeitige als auch die geplante technische Ausstattung sowie das Strafverfolgungs- und Gefahrenabwehrpotenzial dieser Behörden zulassen.

Ferner berühren diese Fragen unmittelbar Aspekte zu technischen Vorgehensweisen und Fähigkeiten der polizeilichen und nachrichtendienstlichen Behörden auf dem Gebiet der informationstechnischen Überwachung. Durch ein Bekanntwerden dieser Methoden könnten die Fähigkeiten der Sicherheitsbehörden mit polizeilichen und nachrichtendienstlichen Aufgaben, Erkenntnisse im Wege der technischen Strafaufklärung und Gefahrenabwehr zu gewinnen, in erheblicher Weise negativ beeinflusst werden, insbesondere, wenn keine ausreichenden Alternativen zu den für die Strafverfolgung und Gefahrenabwehr genutzten Produkten zur Verfügung stehen. Denn Personen könnten sich somit gezielt eben jener Maßnahmen entziehen, etwa durch Aktivitäten zur Hinderung des Einsatzes der entsprechenden Software. Dies ist jedoch nicht hinnehmbar, da die Gewinnung von Informationen durch eine IT- bzw. softwaregestützte Strafverfolgung und Gefahrenabwehr für die Aufgabenerfüllung dieser Behörden und damit für die Sicherheit der Bundesrepublik Deutschland und bei der Bekämpfung vor allem des Terrorismus, der politisch motivierten sowie der organisierten Kriminalität, unerlässlich ist. Sofern solche Informationen entfallen oder wesentlich zurückgehen sollten, würden empfindliche Informationslücken auch im Hinblick auf die Sicherheitslage der Bundesrepublik Deutschland drohen.

Dies würde folgenschwere Einschränkungen der Strafverfolgung und Gefahrenabwehr bedeuten, womit letztlich die gesetzlichen Aufträge von BKA – verankert im Grundgesetz (Artikel 73 Absatz 1 Nummer 9a, Nummer 10 GG, Ar-

tikel 87 GG) und im Bundeskriminalamtgesetz (BKAG), BPOL (Artikel 87 GG und Bundespolizeigesetz (BPolG)) und Zollfahndungsdienst FIU (Artikel 87 GG und Zollfahndungsdienstgesetz (ZFdG), Geldwäschegesetz (GwG), Unionszollkodex (UZK)) – nicht mehr sachgerecht erfüllt werden könnten.

Auch birgt eine Offenlegung der angefragten Informationen die Gefahr, dass Einzelheiten zur konkreten Methodik und zu aus den vorgenannten Gründen im hohen Maße schutzwürdigen spezifischen Fähigkeiten der Nachrichtendienste des Bundes bekannt würden. Infolgedessen könnten sowohl staatliche als auch nichtstaatliche Akteure Rückschlüsse auf spezifische Vorgehensweisen und Fähigkeiten der Nachrichtendienste des Bundes gewinnen. Dies würde folgenschwere Einschränkungen der Informationsgewinnung bedeuten, womit letztlich der gesetzliche Auftrag der Nachrichtendienste des Bundes (§ 1 Absatz 2 BNDG, § 3 Absatz 1 BVerfSchG, § 1 Absatz 1 und § 14 Absatz 1 MADG) nicht mehr sachgerecht erfüllt werden könnte.

Auch eine VS-Einstufung und Hinterlegung der angefragten Informationen in der Geheimschutzstelle des Deutschen Bundestages würde ihrer erheblichen Brisanz im Hinblick auf die Bedeutung der Informationen sowohl für die Aufgabenerfüllung der Nachrichtendienste des Bundes als auch der Sicherheitsbehörden des Bundes mit polizeilichen Aufgaben nicht ausreichend Rechnung tragen, weil insoweit auch ein geringfügiges Risiko des Bekanntwerdens unter keinen Umständen hingenommen werden kann.

Im Ergebnis kommt die Bundesregierung im Rahmen ihrer Abwägung zwischen Staatswohl und parlamentarischem Informationsrecht zu der Einschätzung, dass auch vom Bundestag ergriffene Geheimschutzmaßnahmen den Belangen des Staatswohls nicht hinreichend Rechnung tragen können, weil auch ein geringfügiges Risiko des Bekanntwerdens der betreffenden Informationen unter keinen Umständen hingenommen werden kann, kann die Beantwortung ausnahmsweise verweigert werden (vgl. BVerfGE 124, 78 [138f]). Schon die Angabe, mittels welcher technischen Produkte die Sicherheitsbehörden z. B. von der Telekommunikationsüberwachung Gebrauch machen, könnte zu einer Änderung des Kommunikationsverhaltens der betreffenden beobachteten Personen führen, die eine weitere Aufklärung der von diesen verfolgten Bestrebungen und Planungen unmöglich machen würde. In diesem Fall wäre ein Ersatz durch andere Instrumente nicht möglich.

Aus dem Vorgesagten ergibt sich für die Fragen 1, 2, 3, 4, 14 und 16, dass die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht überwiegt. Insofern muss ausnahmsweise das Fragerecht der Abgeordneten gegenüber den Geheimhaltungsinteressen der Sicherheitsbehörden des Bundes zurückstehen.

1. Kann die Bundesregierung die Medienberichte über Treffen, Produktpräsentationen und Verkaufsgespräche zwischen NSO-Vertretern und Vertretern deutscher Sicherheitsbehörden bestätigen, und wenn ja, wann fanden diese jeweils statt (bitte entsprechend nach Datum, Behörde und Thema des Treffens auflisten)?

Zur Wahrnehmung ihrer Aufgaben hinsichtlich der Weiterentwicklung von Cyberfähigkeiten im Bereich der Informationstechnischen Überwachung steht die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) seit 2018 mit Vertretern der NSO Group Technologies Limited in Kontakt, um im Rahmen einer Marktsichtung Informationen über das Portfolio des Unternehmens zu erhalten und dessen Eignung für eine mögliche Verwendung durch die Si-

cherheitsbehörden des Bundes zu evaluieren. Darüber hinaus wird auf die Vorbemerkung der Bundesregierung verwiesen.

2. Haben nach Kenntnis der Bundesregierung deutsche Sicherheitsbehörden Produkte der Firma NSO Group erworben, und wenn ja, um welche Sicherheitsbehörden und Produkte handelt es sich dabei (bitte entsprechend nach Sicherheitsbehörde, Produkt, Kostenaufwand und Anzahl der Einsätze aufführen)?

3. Wurden deutschen Sicherheitsbehörden von der Firma NSO Group Produkte und/oder Leistungen für Testzwecke (z. B. zeitlich terminierte Testversionen) übermittelt?

   Wenn ja, in welchem Umfang, und über welchen Zeitraum?

   Wurden besagte Testversionen dann auch ausgeführt?

4. Sofern die Spionagesoftware „Pegasus“ zwar von deutschen Behörden beschafft, aber bislang nicht eingesetzt wurde, worin bestanden bzw. bestehen die Gründe?

Die Fragen 2 bis 4 werden gemeinsam beantwortet.

Es wird auf die Vorbemerkung der Bundesregierung verwiesen.

5. Hat die Bundesregierung einen Einsatz der Spionagesoftware „Pegasus“ in Deutschland in rechtlicher Hinsicht bewertet, und wenn ja, mit welchem Ergebnis?

6. Hat die Bundesregierung den Betrieb von Servern der Firma NSO Group in Deutschland zur weltweiten Anwendung der Spionagesoftware „Pegasus“ in rechtlicher Hinsicht bewertet, und sieht sie ggf. Handlungsbedarf (bitte begründen)?

7. Stellen nach Rechtsauffassung der Bundesregierung das Anbieten und der Verkauf der Spionagesoftware „Pegasus“ in Deutschland Straftatbestände nach dem Strafgesetzbuch (StGB) oder nach anderen Rechtsnormen dar, und wenn ja, welche (bitte begründen)?

Die Fragen 5 bis 7 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Das deutsche Recht normiert den jeweiligen Einsatz zur Telekommunikationsüberwachung bzw. zur Onlinedurchsuchung technikneutral. Der Einsatz ist nur im Einzelfall und unter strengen rechtlichen Auflagen zum Schutz hochrangiger Rechtsgüter oder der Verfolgung schwerer bzw. besonders schwerer Straftaten zulässig. Die Zulässigkeitsvoraussetzungen ergeben sich im Einzelnen aus den jeweiligen Rechtsgrundlagen (vgl. etwa zur Quellen-Telekommunikationsüberwachung § 100a Absatz 1 Satz 2, 3 StPO, §§ 5, 51 Absatz 2 BKAG bzw. § 11 Absatz 1a G 10 und zur Onlinedurchsuchung § 100b StPO bzw. § 49 BKAG).

Der Einsatz sogenannter Spähsoftware in Deutschland durch Unberechtigte kann hingegen, je nach den Umständen des Einzelfalls, verschiedene Straftatbestände erfüllen.

Wenn Endgeräte betroffener Personen ausgelesen oder ihre Telefonate abgehört werden, kommen insbesondere die Straftatbestände der Verletzung der Vertraulichkeit des Wortes (§ 201 StGB), des Ausspähens oder Abfangens von Daten (§§ 202a, 202b StGB), des Vorbereitens des Ausspähens und Abfangens von

Daten (§ 202c StGB) oder der Datenhehlerei (§ 202d StGB) in Betracht, wenn die jeweils weiteren Tatbestandsvoraussetzungen gegeben sind. Je nach zu Grunde liegender Planung des Einsatzes sogenannter Spähsoftware und je nach Zielgruppe können auch Straftaten aus dem Bereich des Staatsschutzes, wie § 98 StGB (Landesverräterische Agententätigkeit) und § 99 StGB (Geheimdienstliche Agententätigkeit) vorliegen. Das Anbieten oder Verkaufen von Software, die dem Ausspähen von Daten dient, kann zudem, soweit nicht bereits eine Strafbarkeit nach § 202c StGB gegeben ist, eine strafbare Beihilfehandlung (§ 27 StGB) darstellen, wenn die jeweils weiteren Tatbestandsvoraussetzungen gegeben sind. Künftig kann darüber hinaus bestraft werden, wer eine Handelsplattform im Internet betreibt, deren Zweck darauf ausgerichtet ist, die Begehung bestimmter rechtswidriger Taten zu ermöglichen oder zu fördern (§ 127 StGB-neu). Hierzu gehören auch rechtswidrige Taten nach den §§ 202a bis 202d StGB. Ermittlung und Bewertung eines entsprechenden Sachverhalts sind Angelegenheit der Strafverfolgungsbehörden.

Darüber hinaus beurteilt sich das Anbieten und der Verkauf von Software nach den vertragsrechtlichen Vorschriften des Bürgerlichen Gesetzbuches und verstößt nicht per se gegen die guten Sitten und erfüllt keinen Straftatbestand.

8. Hat die Bundesregierung einen Einsatz der Spionagesoftware „Pegasus“ in Deutschland im Hinblick auf eine Gefährdung der grundrechtlich geschützten Meinungs-, Informations-, Presse-, Rundfunk- und Filmfreiheit (Artikel 5 Absatz 1 und 2 GG) bewertet, und wenn ja, mit welchem Ergebnis (bitte begründen)?

Eingriffe in die grundrechtlich geschützte Meinungs-, Informations-, Presse-, Rundfunk- und Filmfreiheit bedürfen immer einer gesetzlichen Grundlage (z. B. Befugnisnorm aus der Strafprozessordnung oder dem Gefahrenabwehrrecht) und sind nur bei strikter Wahrung der Verhältnismäßigkeit verfassungsrechtlich zulässig. Ermächtigt der Gesetzgeber Behörden zu Maßnahmen der informationstechnischen Überwachung, sind zudem die Vorgaben des Fernmeldegeheimnisses (Artikel 10 GG) einzuhalten.

Hiernach sind die jeweils gesetzlich normierten Voraussetzungen und Verfahrensvorschriften (z. B. Richtervorbehalt) unter strenger Beachtung der Vorgaben des Bundesverfassungsgerichts anzuwenden.

Im Übrigen wird auf die Antwort zu den Fragen 5 bis 7 verwiesen.

9. Haben die Bundesregierung und deutsche Sicherheitsbehörden Kenntnis über die Ausspähung in der Bundesrepublik Deutschland lebender Journalistinnen und Journalisten, Politikerinnen und Politikern oder Menschenrechtsaktivistinnen und Menschenrechtsaktivisten mithilfe der Spionagesoftware „Pegasus“, wenn ja,

   a) durch wen erfolgt die Überwachung,

   b) wer ist davon betroffen,

   c) seit wann besitzt die Bundesregierung diese Informationen,

   d) wurden die zuständigen parlamentarischen Kontrollgremien des Deutschen Bundestages davon in Kenntnis gesetzt, falls nein, weshalb nicht,

   e) wurden Betroffene seitens deutscher Sicherheitsbehörden informiert, und wenn ja, wann, und wenn nein, warum nicht?

Die Fragen 9 bis 9e werden gemeinsam beantwortet.

Der Bundesregierung liegen hierzu keine Erkenntnisse im Sinne der Fragestellung vor.

10. Hat die Bundesregierung überprüft, ob Angehörige der Bundesregierung selbst von Überwachungsmaßnahmen betroffen sind, weil diese in direktem Austausch bzw. Kontakt mit überwachten ausländischen Regierungsangehörigen standen (inklusive Staats- und Regierungschefs, beispielsweise Emmanuel Macron), und wenn ja, mit welchem Ergebnis, und gab es in diesem Zusammenhang Konsultationen mit anderen Regierungen?

Der Bundesregierung liegen hierzu keine Erkenntnisse im Sinne der Fragestellung vor.

11. Ist der Bundesregierung bekannt, ob unter Einsatz von Spionageprodukten der Firma NSO Group auch Rechner und Informationssysteme von an Asylverfahren beteiligten Einrichtungen, vor allem des Bundes, Ziel der Ausspähung durch Geheimdienste von Staaten sind, die Oppositionelle verfolgen?

a) Sind der Bundesregierung derartige Angriffe bekannt, und wenn ja, auf welche Einrichtungen sind diese wann, von wem und mit welchem Ziel jeweils erfolgt, und welche Konsequenzen seitens der Sicherheitsbehörden, des Bundesamts für Sicherheit in der Informationstechnik oder des Verfassungsschutzes hatte dies jeweils?

Wenn nein, haben die Bundesregierung und deutsche Sicherheitsbehörden eine mögliche Ausspähung untersucht, oder werden sie eine solche Untersuchung veranlassen?

b) Sind der Bundesregierung grundsätzlich Angriffe auf die Kommunikationsinfrastruktur des Bundes bzw. in Deutschland bekannt, die mit Produkten der Firma NSO Group verübt wurden?

Wenn ja, welche sind dies, und wie wurde darauf seitens der Sicherheitsbehörden reagiert?

Die Fragen 11 bis 11b werden gemeinsam beantwortet.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) prüft regelmäßig auf Basis von § 5 BSIG Cyberangriffe gegen die Bundesverwaltung. Hinweise zum Einsatz von Überwachungsprodukten der Firma NSO-Group sind in diesem Zusammenhang bisher nicht festgestellt worden. Darüber hinaus liegen der Bundesregierung keine Erkenntnisse im Sinne der Fragestellungen vor.

12. Wie beabsichtigt die Bundesregierung, ihrer Schutzpflicht gegenüber ihren Bürgerinnen und Bürgern, aber auch gegenüber ausländischen Betroffenen (z. B. Journalisten, Menschenrechtsaktivisten und Asylsuchenden) in Deutschland nachzukommen und sie vor Zugriffen ausländischer Geheimdienste zu schützen?

Das BSI fördert den sicheren Einsatz von Informations- und Kommunikationstechnik in Staat, Wirtschaft und Gesellschaft. Als Cyber-Sicherheitsbehörde des Bundes setzt sich das BSI zum Schutz der Bürgerinnen und Bürger unter anderem für die Etablierung grundlegender Sicherheitsstandards und die Information sowie Sensibilisierung der Bürgerinnen und Bürger ein.

Dies umfasst wichtige Sicherheitsempfehlungen, Informationen zu aktuellen Sicherheitsrisiken bzw. Angriffsmethoden sowie Kontakt- und Beteiligungsmöglichkeiten (siehe: https://www.bsi.bund.de/VerbraucherInnen). Insbesonde-

re die Förderung von Verschlüsselungstechniken ermöglicht, dass Bürgerinnen und Bürger in Deutschland kommunizieren können, ohne dass diese Kommunikation auf der Verbindungsstrecke abgehört werden kann. Weiterhin veröffentlicht das BSI Hinweise und Warnungen, mit denen auch Bürgerinnen und Bürger ihre IT-Systeme besser gegenüber Angriffen schützen können. Und schließlich informiert das BSI täglich Betroffene in Deutschland darüber, falls auf ihren IT-Systemen Schadprogramme installiert sind.

13. Was hat die Bundesregierung bislang zum Schutz der Bevölkerung vor Ausspähung durch Spionagesoftware auf deutscher und europäischer Ebene unternommen, und wie ist der aktuelle Umsetzungsstand beim staatlichen Schwachstellenmanagement (Vulnerability Equities Process – VEP)?

Bei Bekanntwerden von Angriffskampagnen mit Relevanz für die IT-Sicherheit in Deutschland informiert das BSI, unabhängig von der Art des Cyber-Angriffs, seine Zielgruppen. Im Rahmen der Veröffentlichungen zu Pegasus hat das BSI am 27. Juli 2021 eine öffentliche Cyber-Sicherheitswarnung mit dem Titel „Smartphones weltweit von Pegasus überwacht“ (CSW-Nr. 2021-234348-1032) herausgegeben https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-234348-1032_csw.html.

Die Bundesregierung setzt sich weiterhin inhaltlich mit dem verantwortungsvollen Umgang mit Schwachstellen auseinander. Eine ausgewogene behördenübergreifende Strategie zum Umgang mit 0-day-Schwachstellen nach den jeweils geltenden gesetzlichen Vorgaben bei den Strafverfolgungs- und Sicherheitsbehörden über bereits vorhandene interne Behördenvorgaben hinaus bringt die Interessen der Cyber- und Informationssicherheit sowie der Strafverfolgungs- und Sicherheitsbehörden in einen angemessenen Ausgleich. Diese Thematik hat auch Eingang in die Cybersicherheitsstrategie Deutschland 2021 gefunden.

14. Wie hoch waren seit 2017 die Kosten für die Entwicklung bzw. die Beschaffung und den Einsatz von Überwachungssoftware von Bundessicherheitsbehörden (bitte entsprechend nach Jahr, Behörde, Erwerb, Entwicklung und Einsatz von Überwachungssoftware aufschlüsseln)?

Es wird auf die als „VS – Nur für den Dienstgebrauch“ eingestufte Anlage 1* gemäß der Vorbemerkung der Bundesregierung verwiesen.

Darüber hinaus wird auf die Vorbemerkung der Bundesregierung verwiesen.

15. Wie hoch waren seit 2017 die Kosten für die Entwicklung bzw. die Beschaffung und den Einsatz von Verschlüsselungs- und Antivirensoftware durch Bundesbehörden (bitte entsprechend nach Jahr, Behörde, Beschaffung, Entwicklung und Einsatz von Verschlüsselungs- und Antivirensoftware aufschlüsseln)?

Es wird auf die als „VS – Nur für den Dienstgebrauch“ eingestufte Anlage 2* gemäß der Vorbemerkung der Bundesregierung verwiesen.

Ferner wird darauf hingewiesen, dass die Kosten für die Entwicklung bzw. die Beschaffung und den Einsatz von Verschlüsselungs- und Antivirensoftware

* Das Bundesministerium des Innern, für Bau und Heimat hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

aufgrund von verschiedenen IT-Komponenten, einer komplexen IT-Infrastruktur, kontinuierlicher (Weiter-)Entwicklung von IT-Fachverfahren, bei denen die Kosten anteilig in den Gesamtentwicklungskosten enthalten sind, sowie nicht aufschlüsselbarer Gesamtkostenmodelle nicht immer ermittelbar sind. Bei nicht eindeutig aufschlüsselbaren Kosten wurden diese teilweise nicht berücksichtigt.

Analog gilt für interne und externe Personalkosten, dass diese dem Betrieb der zu betrachtenden Softwarelösungen nicht immer hinreichend eindeutig zugeordnet werden können. Zu beachten ist auch, dass eingesetzte Software teilweise zentral für verschiedene Behörden finanziert wird und somit die Ausgaben nicht trennscharf den einzelnen Behörden zuzuordnen sind.

Zusammengefasst: Infolge der Komplexität moderner IT-Sicherungssysteme ist eine eindeutige Kostenzuordnung zu den erfragten Softwareprodukten bzw. Sicherungsfunktionen nur eingeschränkt möglich bzw. nur mit unverhältnismäßig hohem Aufwand zu realisieren.

Mit dem Ziel einer weitestgehend konsistenten Datenerhebung wurde diese daher vorrangig auf die bei den Endgeräten zum Einsatz kommende Software fokussiert.

Soweit Angaben zu einzelnen Behörden fehlen, ist dies keinesfalls mit fehlenden Sicherungsmaßnahmen gleichzusetzen. Vielmehr verfügen diese Behörden über keine eigene Informations- und Kommunikationstechnik oder setzen bei Verschlüsselung Antivirensoftwarelizenz- bzw. kostenfreie Produkte ein. Beim BMVg hingegen werden die angefragten Detailinformationen nicht in einer für die Erhebung erforderlichen Form vorgehalten, weshalb hier im Hinblick auf den erheblichen Aufwand von einer gesonderten Erhebung abgesehen wird.

16. Kann die Bundesregierung ausschließen, dass die von Einrichtungen des Bundes entwickelten bzw. geheim gehaltenen Sicherheitslücken von der NSO Group Technologies für ihre Produkte und/oder Leistungen verwendet werden, um weltweit elektronische Geräte zu kompromittieren (bitte begründen)?

Bisher wurden für den Umgang mit Schwachstellen bereits Prozesse bezüglich der Meldung innerhalb der Bundesverwaltung an das BSI und durch das BSI etabliert (vgl. § 4 Absatz 2 bis 4 BSIG). Demnach müssen grundsätzlich alle Bundesbehörden Informationen im Zusammenhang mit neu festgestellten Schwachstellen, die für die Erfüllung von Aufgaben oder die Sicherheit der Informationstechnik anderer Behörden von Bedeutung sind, an das BSI melden.

Gefundene Schwachstellen werden über das BSI dem betroffenen Hersteller gemeldet, damit dieser die Möglichkeit erhält, die Schwachstelle zu schließen. Das Verfahren zielt darauf ab, den durch eine mögliche Ausnutzung von Schwachstellen resultierenden Schaden zu minimieren, da zum einen durch die koordinierte Beteiligung betroffener Hersteller eine Bereitstellung von funktionierenden Sicherheitsupdates ermöglicht wird und zum anderen das temporäre Zurückhalten von Schwachstellen- und Angriffsdetails die Ausnutzung zunächst erschwert und damit das Schadenspotential reduziert werden kann. Als bewährte Methode, sowohl national wie auch international wird der „Coordinated Vulnerability Diclosure“ (CVD) Prozess anerkannt.

Des Weiteren wird auf die Vorbemerkung der Bundesregierung verwiesen.

17. Kennt die Bundesregierung die Forderung des Whistleblower Edward Snowden nach einem Moratorium für den Handel mit Cyberwaffen (vgl. https://www.zeit.de/digital/2021-07/edward-snowden-spionage-software-pegasus-handy-ueberwachung-diktaturen), und hat sie eine Position dazu?

    Wird sie diese Forderung umsetzen?

    Wenn nein, warum nicht?

18. Kennt die Bundesregierung die Forderung des Deutschen Journalisten-Verbandes (DJV), die deutschen Sicherheitsbehörden und die Geheimdienste sollen Auskunft darüber geben, ob die „Pegasus"-Spähsoftware gegen deutsche Journalistinnen und Journalisten eingesetzt wurde (https://www.djv.de/startseite/profil/der-djv/pressebereich-download/pressemitteilungen/detail/news-aufklaerung-gefordert-2), und wird sie darauf reagieren?

    Wenn ja, in welcher Form (bitte begründen)?

19. Wie hat oder wird die Bundesregierung auf die Forderung der Vereinten Nationen nach einer menschenrechtszentrierten Regulierung solcher Überwachungssoftware reagieren (https://news.un.org/en/story/2021/07/1096142; bitte begründen)?

Die Fragen 17 bis 19 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Über die mediale Berichterstattung hinaus liegen der Bundesregierung hierzu keine Informationen im Sinne der Fragestellung vor.

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