Deutscher Bundestag **Drucksache 19/25579**

19. Wahlperiode 23.12.2020

Kleine Anfrage

der Abgeordneten Dr. Irene Mihalic, Dr. Konstantin von Notz, Kordula Schulz-Asche, Dr. Tobias Lindner, Luise Amtsberg, Margarete Bause, Canan Bayram, Dr. Franziska Brantner, Agnieszka Brugger, Dr. Janosch Dahmen, Kai Gehring, Britta Haßelmann, Uwe Kekeritz, Katja Keul, Maria Klein-Schmeink, Omid Nouripour, Cem Özdemir, Filiz Polat, Tabea Rößner, Claudia Roth (Augsburg), Manuel Sarrazin, Ulle Schauws, Dr. Frithjof Schmidt, Charlotte Schneidewind-Hartnagel, Margit Stumpp, Jürgen Trittin, Ottmar von Holtz und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Schutz der Produktion, Verteilung und Abgabe der COVID-19-Impfstoffe

Die Europäische Arzneimittelbehörde EMA soll nach Medienberichten am 21. Dezember 2020, sechs Tage früher als ursprünglich geplant, die Zulassung des COVID-19-Impfstoffs des Unternehmens Biontech für den Einsatz in Europa bescheiden. Damit steht auch in Aussicht, dass noch in diesem Jahr auch in Deutschland mit den Impfungen gegen das Virus SARS-CoV-2 begonnen werden kann (vgl. tagesschau.de vom 15. Dezember 2020 „Impfstoff-Entscheidung“ am 21. Dezember abrufbar unter: https://www.tagesschau.de/ausland/biontech-zulassung-101.html). Dadurch rückt nach Auffassung der Fragestellerinnen und Fragesteller die Frage der Sicherheit der Einrichtungen und Infrastrukturen zur Produktion, Verteilung und Abgabe der Impfstoffe in den Vordergrund.

Die vergangenen Wochen haben gezeigt, dass es ein regelrechtes, weltweites Wettrennen um die Entwicklung und Zulassung von Impfstoffen gegeben hat. Bereits seit Ende November 2020 warnt das Bundesamt für Sicherheit in der Informationstechnik (BSI) vor einer hohen Bedrohungslage der deutschen Impfstoffherstellerinnen und Impfstoffhersteller. Diese seien ein attraktives Ziel für Angreiferinnen und Angreifer (vgl. Reuters vom 26. November 2020 „BSI besorgt wegen möglicher Cyber-Angriffe auf Impfstoff-Hersteller“, abrufbar unter https://de.reuters.com/article/virus-cyber-bsi-idDEKBN2861J0). Anfang Dezember 2020 warnte auch Interpol vor IT-Angriffen auf europäische Impfstoffhersteller und Logistikketten (vgl. Der Standard vom 2. Dezember 2020 „Impfstoffe: Warnungen vor Cyberangriffen im Gesundheitssektor“, abrufbar unter https://www.derstandard.de/story/2000122177538/impfstoffe-warnungen-vor-cyberangriffen-im-gesundheitssektor).

Neben dem Bundesamt für Sicherheit und Informationstechnik (BSI) und Interpol warnte auch der IT-Konzern IBM bereits vor Manipulation der Kühlketten für Corona-Impfstoffe durch IT-Angriffe. Weltweit seien Phishing-Aktivitäten gegen Organisationen entdeckt worden, die mit den Kühlketten beschäftigt seien, wobei die präzise Ausführung auf eine staatlich gelenkte Aktionen hindeute (vgl. Handelsblatt vom 3. Dezember 2020 „IBM warnt vor Cyberangrif-

fen auf Corona-Impfstoff-Kühlketten“, abrufbar unter: https://www.handelsblatt.com/technik/it-internet/phishing-aktivitaeten-ibm-warnt-vor-cyberangriffen-auf-corona-impfstoff-kuehlketten/26685346.html?ticket=ST-15007682-yhOqZfau29HgmNdw69HG-ap6).

In einem internen Lagebericht soll auch das Bundeskriminalamt (BKA) bereits Ende November 2020 vor Attacken auf Impfstoffherstellerinnen und Impfstoffhersteller sowie Impfzentren gewarnt haben. Für die Transport- und Lagerstätten bestehe eine „abstrakte Gefahr“. Gegnerinnen und Gegner der Anti-Corona-Maßnahmen könnten versuchen, in die Zentren einzudringen. Auch Gewalt sei nicht auszuschließen. Neben dieser Gefährdungslage sei auch nicht auszuschließen, dass es zu Diebstählen oder Angriffen auf die IT-Infrastruktur der Unternehmen durch staatliche Akteurinnen und Akteure oder Konkurrenzunternehmen kommen könnte (vgl. sueddeutsche.de vom 27. November 2020 „BKA warnt vor Attacken auf Impfstoffhersteller und Impfzentren“, abrufbar unter: https://www.sueddeutsche.de/politik/corona-sicherheit-bka-1.5129994).

Bayerns Innenminister Joachim Herrmann (CSU) geht laut Presseberichten davon aus, dass sich die Polizeien von Bund und Ländern arbeitsteilig um die Bewachung der Corona-Impfstoffe kümmern werden. Die Bundespolizei werde den Transport der Impfstoffe bis zu den jeweiligen Zentrallagern in den Ländern bewachen. Für die sichere Verteilung des Impfstoffe innerhalb der Länder seien dann die Polizeibehörden der Länder verantwortlich (vgl. RND vom 10. Dezember 2020 „Herrmann: Bundespolizei soll an Impfstoff-Bewachung beteiligt sein“, abrufbar unter: https://www.rnd.de/politik/herrmann-bundespolizei-soll-an-impfstoff-bewachung-beteiligt-sein-H3IDZI2WM2SSJOSOXSPENOTGWM.html).

Nach Auffassung der Fragestellerinnen und Fragesteller sind diese Warnungen sehr ernst zu nehmen. Gerade die fortschreitende Radikalisierung und zunehmende Unterwanderung der Proteste gegen die Anti-Corona-Maßnahmen von Bund und Ländern durch Akteurinnen und Akteure aus dem antisemitischen, rechtsextremen sowie verschwörungsideologischen Spektrum lassen auf eine mindestens abstrakte, wenn nicht sogar konkrete, Gefährdung dieser Einrichtungen schließen (vgl. Zeit Online vom 1. Dezember 2020 „Mit weiterer Gewalt ist zu rechnen“, abrufbar unter: https://www.zeit.de/politik/deutschland/2020-12/corona-demos-extremismus-verfassungsschutz-bka-rki-brandanschlag-sprengstoffanschlag?utm_referrer=https%3A%2F%2Fwww.google.com%2F), nicht zuletzt, weil Impfmythen einen zentralen Bestandteil der Verschwörungserzählungen ausmachen (vgl. welt.de vom 17. November 2020 „Jetzt radikalisieren sich die Impfgegner“, abrufbar unter: https://www.welt.de/politik/deutschland/article220259232/Verschwoerungsideologien-Jetzt-radikalisieren-sich-die-Impfgegner.html).

Die Warnungen bezüglich digitaler Bedrohungen haben sich mittlerweile bestätigt: Während sich die IT-Systeme der Unternehmen als sicher erwiesen haben, wurde in das IT-System der europäischen Arzneimittelbehörde EMA bereits erfolgreich von außen eingedrungen. Im Zuge des Angriffs, der am frühen Morgen des 1. Dezember 2020 entdeckt wurde, gelang es, sich unberechtigten Zugang zu Daten zu verschaffen – darunter auch Informationen zu den COVID-19-Impfstoffen der Unternehmen Moderna sowie Pfizer/Biontech. Die Unternehmen sollen erst mit tagelanger Verspätung von dem Vorfall in Kenntnis gesetzt worden sein. Mittlerweile liegen auch deutschen Sicherheitsbehörden, unter anderem dem BSI, die bisherigen Erkenntnisse der niederländischen Ermittlungsbehörden vor. Demnach werde davon ausgegangen, dass es sich bei den Angreiferinnen und Angreifern mutmaßlich um staatliche Akteurinnen und Akteure handele. Darauf ließen Vorgehensweise und eingesetzte Schad-Software schließen (vgl. tagesschau.de vom 17. Dezember 2020 „Cyberattacke auf

die EMA – War es ein Geheimdienst?“, abrufbar unter: https://www.tagesschau.de/investigativ/wdr/pfizer-biontech-ema-cyberattacke-103.html).

Wir fragen die Bundesregierung:

1. Wie bewertet die Bundesregierung die aktuelle Gefährdungslage für Einrichtungen zur Impfstoffforschung, Impfstoffproduktion oder Impfstoffzulassung der COVID-19-Impfstoffe?
2. Inwiefern sind der Bundesregierung bisher sicherheitsrelevante Sacherhalte im Zusammenhang mit der Impfstoffforschung sowie Impfstoffproduktion der COVID-19-Impfstoffe bekannt geworden?
3. Wie beurteilt die Bundesregierung die Gefährdungslage für Einrichtungen zur Lagerung, Verteilung sowie Abgabe der COVID-19-Impfstoffe (insbesondere von geplanten Impfzentren)?
4. Wie bewertet die Bundesregierung die Gefährdungslage dieser Einrichtungen und Infrastrukturen insbesondere im Hinblick auf Bedrohungen im Bereich der politisch motivierten Kriminalität?
5. Wie bewertet die Bundesregierung die Gefährdungslage dieser Einrichtungen und Infrastrukturen insbesondere im Hinblick auf Bedrohungen im Bereich von staatlichen IT-Angriffen?
6. Inwiefern sind der Bundesregierung Aufrufe, Planungen, Erwägungen oder Vernetzungen mit Zielsetzung der Sabotage oder anderer Störaktionen gegenüber Einrichtungen oder Infrastrukturen der Impfstoffherstellung, Impfstoffabgabe oder des Impfstofftransports aus dem antisemitischen, rechtsextremen sowie dem verschwörungsideologischen oder des sogenannten „Querdenken“-Spektrums bekannt?
7. Inwiefern erlangte die Bundesregierung im Rahmen des offenen Internetmonitorings von Telegram-Kanälen und weiteren offenen zugänglichen Gruppen und Seiten in sozialen Medien, die zur Vernetzung der sogenannten „Querdenken“-Bewegung genutzt werden (vgl. Antwort zu Frage 10 auf Bundestagsdrucksache 19/19785), Erkenntnisse über Aufrufe Planungen, Erwägungen oder Vernetzungen mit Zielsetzung von Angriffen auf die Infrastrukturen zur Impfstoffherstellung, Impfstoffabgabe und Impfstofftransport (vgl. sueddeutsche.de vom 27. November 2020 „BKA warnt vor Attacken auf Impfstoffhersteller und Impfzentren“, abrufbar unter: https://www.sueddeutsche.de/politik/corona-sicherheit-bka-1.5129994)?
8. Wie beurteilt die Bundesregierung insbesondere die Sicherheit der in den Impfzentren tätigen Personen?
9. Wie beurteilt die Bundesregierung die Sicherheit der zukünftigen Patientinnen und Patienten der Impfzentren?
10. Inwiefern sind die Polizeien sowie andere Sicherheitsbehörden des Bundes (Bundeskriminalamt, Bundespolizei, Bundesamt für Verfassungsschutz, Bundesamt für Sicherheit in der Informationstechnik) bei der Sicherung von Einrichtungen und Infrastrukturen der Impfstoffherstellung, Impfstoffabgabe oder des Impfstofftransports eingebunden, bzw. welche Planungen gibt es diesbezüglich?
11. Inwiefern wurden bereits Schutzmaßnahmen seitens des Bundes für die Einrichtungen und Infrastrukturen der Impfstoffherstellung, Impfstoffforschung, Impfstoffzulassung, Impfstoffabgabe oder des Impfstofftransports ergriffen bzw. die Länder durch Bundesbehörden bei der Ergreifung von Schutzmaßnahmen beraten?

12. Inwiefern sind Medienberichte zutreffend, dass die Bundespolizei die Impfstofftransporte absichern soll (vgl. Zeit Online vom 10. Dezember 2020 „Herrmann: Polizei soll Impfstoff bewachen“, abrufbar unter: https://www.zeit.de/news/2020-12/10/herrmann-polizei-soll-impfstoff-bewachen?utm_referrer=https%3A%2F%2Fwww.google.com%2F)?

13. Inwiefern sind Medienberichte zutreffend, dass die COVID-19-Impfstoffe zentral in einer Bundeswehrkaserne in Quakenbrück gelagert werden soll (vgl. NDR vom 14. Dezember 2020 „Corona-Impfstoffe: Bundesweites Zentrallager in Quakenbrück?“, abrufbar unter https://www.ndr.de/nachrichten/niedersachsen/osnabrueck_emsland/Corona-Impfstoffe-Bundesweites-Zentrallager-in-Quakenbrueck,zentrallager102.html)?

    a) Inwiefern ist ein zentrales Depot zur Lagerung der Impfstoffe aus sicherheitspolitischer Perspektive nach Auffassung der Bundesregierung sinnvoll?

    b) Inwiefern wird die Bundeswehr für die Sicherung der Impfstoffe verantwortlich sein, und inwiefern sind Soldatinnen und Soldaten bei der Impfstoffverteilung eingebunden?

    c) Inwiefern sind der Bundesregierung gezielte Planungen und Aufrufe zu geplanten Störungen und Angriffen auf die Bundeswehrkaserne in Quakenbrück im Zusammenhang mit der Impfstofflagerung bekannt?

14. Welche Kenntnisse liegen der Bundesregierung und/oder ihr nachgeordneten Behörden bezüglich versuchter bzw. erfolgreicher Angriffe und erhöhter Gefährdungslagen durch IT-Angriffe auf Unternehmen und Infrastrukturen zur Impfstoffherstellung, Impfstoffforschung, Impfstoffzulassung, Impfstoffabgabe oder des Impfstofftransports vor, und welche Akteurinnen und Akteure wurden als besondere Bedrohung identifiziert?

15. Auf welche konkreten Erkenntnisse bezogen sich beispielsweise die Warnungen des Bundesamts für Sicherheit in der Informationstechnik Ende November 2020 (vgl. Reuters vom 26. November 2020 „BSI besorgt wegen möglicher Cyber-Angriffe auf Impfstoff-Hersteller“, abrufbar unter https://de.reuters.com/article/virus-cyber-bsi-idDEKBN2861J0)?

16. Auf welche konkreten Erkenntnisse bezogen sich beispielsweise die Warnungen des Bundesamts für Sicherheit in der Informationstechnik vom 17. Dezember 2020 (vgl. BR vom 17. Dezember 2020 „Bundesamt warnt vor Cyber-Angriffen auf Impfstoff-Versorgung“, abrufbar unter https://www.br.de/nachrichten/meldung/bundesamt-warnt-vor-cyberangriffen-auf-impfstoff-versorgung,300351d3a)?

17. Welche Gespräche sowie „Informations- und Sensibilisierungsmaßnahmen“ haben zwischen Sicherheitsbehörden im Verantwortungsbereich der Bundesregierung sowie dem Bundesamt für Sicherheit in der Informationstechnik (BSI) mit den Herstellerinnen und Herstellern von Impfstoffen stattgefunden, um diese auf Gefährdungslagen durch IT-Angriffe hinzuweisen, und welche konkreten Schutzvorkehrungen wurden daraufhin ergriffen (bitte konkret mit Datum und Unternehmen, vgl. Antwort der Bundesregierung auf die Schriftliche Frage 64 Dr. Konstantin von Notz auf Bundestagsdrucksache 19/25435)?

18. Welche konkreten Maßnahmen haben welche Bundesbehörden ergriffen, um die „detaillierte Identifikation aller Beteiligten und Sicherstellung eines einheitlichen Informationsstandes bei den Betroffenen“ sicherzustellen, und wann wird dieser Prozess nach Ansicht der Bundesregierung abgeschlossen sein (vgl. ebd.)?

19. Wie erklärt die Bundesregierung den Umstand, dass sie selbst auf eine Schriftliche Frage am 10. Dezember 2020 antwortete, dass dem Bundesministerium des Innern, für Bau und Heimat (BMI) „keine Erkenntnisse über konkrete Angriffe auf Unternehmen oder Einrichtungen in Deutschland“ vorlägen, während das dem BMI untergeordnete BSI exakt hiervor seit Monaten warnte, und lagen auch dem BSI zum derzeitigen Zeitpunkt keinerlei Kenntnisse auf versuchte oder erfolgreiche IT-Angriffe vor (vgl. ebd.)?

20. Ist der Hinweis in der erwähnten Frage, das BMI habe „keine Erkenntnisse über konkrete Angriffe auf Unternehmen oder Einrichtungen“, die sich allein auf Angriffe „in Deutschland“ bezog (vgl. ebd.) als Bestätigung zu werten, dass die Bundesregierung zu diesem Zeitpunkt bereits über die erfolgreichen Angriffe auf die EMA und den Abfluss von Daten auch deutscher Impfstoffherstellerinnen und Impfstoffhersteller wusste?

21. Teilt die Bundesregierung die Ansicht, dass die Antwort (vgl. ebd.) insofern zumindest irreführend ist, da die Fragestellenden explizit nach Erkenntnissen „über vergangene und verstärkt zu erwartende (Phishing-)Aktivitäten, Manipulationsversuche und IT-Angriffe auf Corona-Impfstoffherstellerinnen und -hersteller sowie Versorgungsketten (mitsamt Lagerung, Lieferung und Kühlung)“ fragten, also explizit nicht ausschließlich nach Angriffen auf deutschem Boden?

22. Würden nach Ansicht der Bundesregierung die Herstellerinnen und Hersteller von Impfstoffen und die digitalen Infrastrukturen der derzeit in Errichtung befindlichen Impfzentren unter die Schutzmechanismen des am 16. Dezember 2020 im Bundeskabinett verabschiedeten Entwurfs eines Zweiten Gesetzes zur Erhöhung der Sicherheit Informationstechnischer Systeme („IT-Sicherheitsgesetz 2.0“, ITSIG 2.0) bzw. bereits vorliegender oder noch zu erarbeitender Verordnungen hierzu fallen (vgl. Antwort der Bundesregierung auf Schriftliche Frage 65 Dr. Konstantin von Notz auf Bundestagsdrucksache 19/25435)?

23. Welche Daten wurden nach Kenntnis der Bundesregierung und/oder ihr nachgeordneter Behörden bei dem Angriff auf die europäischen Arzneimittelbehörde EMA konkret entwendet?

24. Welche möglichen Auswirkungen und ggf. neue Gefährdungslagen könnten sich durch den Umstand, dass offenbar auch Daten zu den einzelnen Impfstoffen erbeutet wurden (vgl. tagesschau.de vom 15. Dezember 2020, a. a. O.), nach Kenntnis der Bundesregierung und/oder ihr nachgeordneter Behörden ergeben?

25. Welche Art des Angriffs auf die europäische Arzneimittelbehörde EMA hat nach Kenntnis der Bundesregierung und/oder ihr nachgeordneter Behörden konkret stattgefunden, und welche Schad-Software bzw. Schadprogramme wurden hierfür nach heutigem Kenntnisstand durch die Angreiferinnen und Angreifer genutzt?

26. Lassen die bisherigen Ermittlungen aus Sicht der Bundesregierung und/oder ihr nachgeordneter Behörden den Schluss zu, dass es sich bei den Angreiferinnen und Angreifer um (teil-)staatliche Akteurinnen und Akteure gehandelt haben könnte, und sollte dies zutreffen, welche Erkenntnisse sind dies konkret?

27. Wann konkret bekamen die Bundesregierung und/oder ihr nachgeordnete Behörden Kenntnis über die erfolgreichen Angriffe auf die europäischen Arzneimittelbehörde EMA?

28. Warum wurden die betroffenen Unternehmen nach Kenntnis der Bundesregierung und/oder ihr nachgeordneter Behörden erst mit tagelanger Verspätung über den Angriff informiert (vgl. tagesschau.de vom 17. Dezember 2020 „War es ein Geheimdienst?“, abrufbar unter https://www.tagesschau.de/investigativ/wdr/pfizer-biontech-ema-cyberattacke-103.html)?

29. Informierten die Bundesregierung und/oder ihr nachgeordnete Behörden die betroffenen Unternehmen selbst oder nahmen nach dem erfolgreichen Angriffen Kontakt zu den Unternehmen auf, falls ja, wann, und mit welchem konkreten Ziel?

30. Welche Kenntnisse liegen der Bundesregierung und/oder ihr nachgeordneten Behörden zu den jüngsten, mindestens seit März 2020 andauernden, weitreichenden IT-Angriffen auf die Regierung der Vereinigten Staaten von Amerika vor, die von US-Behörden als „ernste Gefahr“ für die Bundesregierung, für Regierungen von Bundesstaaten und Kommunen, für die kritische Infrastruktur und für Organisationen des Privatsektors eingeschätzt wird (vgl. tagesschau.de vom 18. Dezember 2020 „US-Behörde warnt vor ‚ernster Gefahr‘“, abrufbar unter https://www.tagesschau.de/ausland/usa-cyberangriff-101.html), und stehen, gerade vor dem Hintergrund der Ankündigung des designierten US-Präsidenten Joe Biden, die Verantwortlichen würden „in Abstimmung mit Verbündeten zur Rechenschaft gezogen“, Bundesregierung und/oder ihr nachgeordnete Behörden mit der US-Regierung und/oder ihr nachgeordneten Behörden wie der Behörde für Cyber- und Infrastruktursicherheit (Cisa) im Austausch, auch bezüglich der konkreten Angriffsart, der verwendeten Schad-Software bzw. Schadprogramme, mutmaßlich hinter dem Angriff stehender (staatlicher oder teils staatlicher) Akteure und möglicher Gegenmaßnahmen?

Berlin, den 22. Dezember 2020

Katrin Göring-Eckardt, Dr. Anton Hofreiter 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