Deutscher Bundestag **Drucksache 19/25996**

19. Wahlperiode 19.01.2021

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Dr. Irene Mihalic, Dr. Konstantin von Notz, Kordula Schulz-Asche, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN
– Drucksache 19/25579 –

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

Vorbemerkung der Fragesteller

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 Cyberangriffen auf Corona-Impfstoff-Kühlketten“, abrufbar unter: https://www.handelsblatt.com/technik/it-internet/phishing-aktivitaeten-ibm-warnt-vor-cy

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 19. Januar 2021 übermittelt.
Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

berangriffen-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).

1. Wie bewertet die Bundesregierung die aktuelle Gefährdungslage für Einrichtungen zur Impfstoffforschung, Impfstoffproduktion oder Impfstoffzulassung der COVID-19-Impfstoffe?

Der Bundesregierung liegen derzeit keine konkreten gefährdungsrelevanten Erkenntnisse im Sinne der Fragestellung vor. Sie geht aufgrund der großen medialen Präsenz sowie der hohen Dynamik und Emotionalität, die dem Themenkomplex „Corona“ innewohnt, von einer abstrakten Gefährdung zum Nachteil der Firmensitze, aber auch der Impfzentren, Impfstoff-Transporte und -Lagerstätten aus. In diesem Zusammenhang sind insbesondere Proteste von Impfgegnern, Corona-Skeptikern und Verschwörungstheoretikern auch an Standorten der Produktionsfirmen, der Impfzentren und der Impfstoff-Lagerstätten einzukalkulieren. Ergänzend ist in Betracht zu ziehen, dass Personen versuchen könnten, in die Impfzentren sowie die Lagerstätten einzudringen, um einerseits Aufmerksamkeit zu erregen und andererseits ihrem Protest Nachdruck zu verleihen. Dies könnte eskalierend mit Sachbeschädigungen in den Gebäuden einhergehen. In Einzelfällen könnte es bei Aufeinandertreffen mit dem beschäftigten Personal oder den Impfempfängern zu auch strafrechtlich relevanten physischen Übergriffen kommen.

Die Gefahr von Cyberangriffen für die in der Frage genannten Einrichtungen und Unternehmen muss derzeit aufgrund des besonderen Fokus, in dem sie im Zusammenhang mit dem Impfstoff stehen, als hoch eingestuft werden. Bis die Corona-Pandemie nicht global eingedämmt worden ist, bleiben sie ein attraktives Ziel für Angriffe, denen sowohl wirtschaftliche als auch staatliche Interessen zugrunde liegen können.

2. Inwiefern sind der Bundesregierung bisher sicherheitsrelevante Sacherhalte im Zusammenhang mit der Impfstoffforschung sowie Impfstoffproduktion der COVID-19-Impfstoffe bekannt geworden?

Aus Sicht der Bundesregierung sind im Sinne der Fragestellung die Cyber-Angriffe auf das Unternehmen Miltenyi Biotec und die Europäische Arzneimittelagentur (EMA) zu nennen. Darüber hinaus berichteten Experten von IBM Anfang Dezember über bereits seit September 2020 laufende, globale Phishing-Angriffe auf Unternehmen, die im Zusammenhang mit der Verteilung von COVID-19-Impfstoffen stehen.

Einzelne Sicherheitsunternehmen haben zudem über angebliche Sabotage gegen Hersteller von Kühlgeräten für Impfstoffe berichtet. Die technischen Analysen in diesen Berichten unterscheiden jedoch nicht ausreichend zwischen ungezielten Angriffen und solchen, die tatsächlich gezielt die Impfstoff-Lieferkette angreifen. Der Bundesregierung ist zudem ein Ransomware-Vorfall in einem Unternehmen, welches an der Entwicklung eines Impfstoffes beteiligt ist, bekannt. Dieser Angriff ist jedoch als ungezielt zu bewerten.

3. Wie beurteilt die Bundesregierung die Gefährdungslage für Einrichtungen zur Lagerung, Verteilung sowie Abgabe der COVID-19-Impfstoffe (insbesondere von geplanten Impfzentren)?

Es wird auf die Antwort zu Frage 1 verwiesen.

4. Wie bewertet die Bundesregierung die Gefährdungslage dieser Einrichtungen und Infrastrukturen insbesondere im Hinblick auf Bedrohungen im Bereich der politisch motivierten Kriminalität?

Es wird auf die Antwort zu Frage 1 verwiesen.

Ergänzend ist zu berücksichtigen, dass Impfzentren und Lagerstätten, aber auch Transporte, grundsätzlich zudem ein Ziel für islamistisch motivierte Täter darstellen können, da insbesondere bei Impfzentren mit einer großen Menschenansammlung zu rechnen ist, denen jihadistische Tätergruppierungen und Einzeltäter eine besonders hohe Bedeutung zumessen.

5. Wie bewertet die Bundesregierung die Gefährdungslage dieser Einrichtungen und Infrastrukturen insbesondere im Hinblick auf Bedrohungen im Bereich von staatlichen IT-Angriffen?

Die Bundesregierung sieht Einrichtungen zur Impfstoffforschung, -produktion oder -zulassung als potentielle Ziele für Spionage und Sabotage durch fremde Nachrichtendienste an. Es sind mehrere mutmaßliche Ausforschungsversuche bezüglich deutscher Impfstoffhersteller bekannt geworden. Aufgrund der Bedeutung und Aktualität dieser Einrichtungen und deren Forschung besteht zudem grundsätzlich die Gefahr von Cyberangriffen mit nachrichtendienstlichem Hintergrund.

Anzeichen für gezielte Sabotage-Angriffe von staatlicher Seite gegen Logistik-Ketten liegen der Bundesregierung nicht vor.

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?

Der Bundesregierung liegen derzeit keine Erkenntnisse zu konkreten Gefährdungen der genannten Einrichtungen vor.

Hinweise auf möglicherweise sicherheitsrelevante Sachverhalte mit Bezug zu Impfzentren konnten auf der Plattform „Telegram“ festgestellt werden. In verschiedenen Regionalgruppen von „D-Day 2.0“ erwägen Nutzer, sich vor Impfzentren zu versammeln. Informationen über die tatsächliche Durchführung solcher Versammlungen liegen nicht vor.

Die Nutzer und Organisatoren in den „D-Day 2.0“- Gruppen und -Kanälen lassen sich dem antisemitischen, rechtsextremen oder dem sogenannten „Querdenken“-Spektrum nicht zuordnen. Ausführungen von „Markus Lowien“, einem Organisator von „D-Day 2.0“, begründen die Annahme, dass er dem verschwörungsideologischen Spektrum zuzuordnen ist. In einem Video vom 21. Dezember 2020 richtet er sich z. B. an Bundeswehrangehörige. In diesem konstatiert er, dass „die Wahrheit verschwiegen“ und dem Volk „massiver Schaden“ zugefügt werde.

Des Weiteren erklärt Attila Hildmann auf seinem Telegram-Kanal, dass die Spritzen in den Impfzentren den Bomben des Bombenhagels von Dresden gleichen. In diesem Zusammenhang führt er aus, dass Versammlungen sinnlos seien. Stattdessen müsse gezielt „gegen das Unrecht“ vorgegangen werden.

Die Sicherheitsbehörden des Bundes beobachten die Entwicklungen in diesem Zusammenhang aufmerksam und stehen in kontinuierlichem Austausch mit den Sicherheitsbehörden der Länder.

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)?

Die genannten Erkenntnisse wurden durch das offene Monitoring von Telegramgruppen und -kanälen durch das Bundeskriminalamt (BKA) erlangt.

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?

Die Fragen 8 und 9 werden gemeinsam beantwortet.

Auf die Antwort zu Frage 1 wird verwiesen.

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?

Die Bundesregierung verweist auf die grundsätzliche Zuständigkeit der Länder, zu deren Maßnahmen und Planungen sie sich nicht äußert.

Vor allem mit Blick auf die herausragende Bedeutung von Einrichtungen und Infrastrukturen der Impfstoffherstellung, -abgabe oder des -transports beobachten die Sicherheitsbehörden des Bundes die Entwicklungen in diesem Zusammenhang aufmerksam und stehen in kontinuierlichem Austausch mit den Sicherheitsbehörden der Länder.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) arbeitet mit den im Sinne der Fragestellung betroffenen Unternehmen auf freiwilliger Basis zusammen. Das BSI hat bei den relevanten Impfstoffherstellern Beratungen durchgeführt und Unterstützungsleistungen dargestellt. Weitergehend erfolgt bei den als besonders kritisch klassifizierten Unternehmen ein unmittelbarer Austausch über potentielle aktuelle Angriffskampagnen und Gefährdungen. Darüber hinaus wurden Erreichbarkeiten im Notfall sichergestellt. Die Unterstützungsleistungen stehen allen als kritisch identifizierten Unternehmen und Institutionen zur Verfügung.

Darüber hinaus wird auf die Antwort zu Frage 11 verwiesen.

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?

Die Bundespolizei schützt auf Grundlage eines Amtshilfeersuchens des Bundesministeriums für Gesundheit vom 24. November 2020 die für Deutschland vorgesehenen Impfstofftransporte ab der Übernahme an der deutschen Grenze bis zu den Verteilzentren der Länder. Hierzu steht die Bundespolizei in engem Austausch mit den Polizeien der Länder sowie den betroffenen Hersteller- und Logistikfirmen. Für eventuell erforderliche Schutzmaßnahmen der landesinternen Transporte sowie der Verteil- und Impfzentren sind die Polizeien der Länder zuständig.

Das Bundesamt für Verfassungsschutz (BfV) hat Impfstoffhersteller – zum Teil gemeinsam mit dem BSI – über die Gefahren durch Spionage und Sabotage in persönlichen Gesprächen oder in entsprechenden Videokonferenzen sensibilisiert. Darüber hinaus wurden Hinweisschreiben des BfV zu Spionage- und Sabotagegefahren über Fachverbände an die relevanten Akteure (Forschungsunternehmen, Unternehmen für klinische Auftragsstudien) versendet. Ein für die Zulassung von Impfstoffen relevantes Institut wurde vom Verfassungsschutz bereits im Mai sensibilisiert; empfohlene Sicherheitsmaßnahmen wurden umgesetzt. In einem weiteren Termin Anfang Dezember wurden – gemeinsam mit dem BSI – noch einmal Prozesse im Hinblick auf Vulnerabilitäten erörtert.

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)?

Auf die Antwort zu Frage 11 wird verwiesen.

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?

Die Fragen 13 und 13a werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Die Verträge der Europäischen Union zum Einkauf der COVID-19-Impfstoffe sehen – mit Ausnahme des Vertrages mit BioNtech – je Mitgliedsstaat eine zentrale Anlieferstelle vor. Da die Bundesregierung keine eigenen Apotheken bzw. logistischen Einrichtungen besitzt, wurde die Bundeswehr um Amtshilfe gebeten, die Impfstofflagerung und Verteilung zu übernehmen. Aufgrund von arzneimittelrechtlichen Anforderungen an das nationale Verteilzentrum (u. a. Qualitätsmanagementsystem, Großhandelserlaubnis) und von Sicherheitsaspekten wurde eine zentrale nationale Hauptumschlagbasis innerhalb eines militärischen Sicherheitsbereich – konkret das Versorgungs- und Instandsetzungszentrum Quakenbrück – gewählt.

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

Die Bundeswehr sichert das Material und Personal innerhalb seiner Liegenschaften mit an die aktuelle Sicherheitslage fortlaufend angepassten Maßnahmen. Hierbei stehen die regional zuständigen Stellen im direkten Kontakt mit den zivilen Sicherheitsorganen.

Angehörige der Bundeswehr betreiben die Lagereinrichtung und organisieren den Versand der Impfstoffe an die Verteilzentren der Bundesländer.

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?

Der Bundesregierung liegen keine Erkenntnisse oder Informationen vor, welche Rückschlüsse auf eine mögliche –besondere- Bedrohung des Versorgungs- und Instandsetzungszentrums Quakenbrück begründen oder darauf hindeuten.

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?

Die Bundesregierung verweist auf ihre Antwort zu Frage 2 und betont erneut, dass Unternehmen und Infrastrukturen im Impfstoffsektor aufgrund ihrer Arbeit zur Bekämpfung der COVID-19-Pandemie potenziell in den Fokus nachrichtendienstlicher Ausspähung gelangen können.

Aus Berichten von Sicherheitsfirmen und Warnungen ausländischer Behörden gehen die Gruppen Kimsuky, APT32 und Lazarus hervor, sowie das Spionage-Programm WellMess. Ein Team der Cybersicherheitsabteilung des Unternehmens IBM hat darüber hinaus Phishing-Angriffe auf ausgewählte Führungspersonen von Unternehmen festgestellt, die im Zusammenhang mit der Verteilung der Impfstoffe gegen COVID-19 stehen. Die Angriffe laufen demnach seit September 2020. Ziel seien Firmen, Organisationen und Behörden im Umfeld der Impf-Allianz Gavi beziehungsweise deren Initiative Cold Chain Equipment Optimisation Platform (CCEOP) für eine Verbesserung der Kühlkette gewesen. Um die Phishing-Mails für die Empfänger glaubwürdig aussehen zu lassen, hätten die Angreifer als Absender der E-Mail das chinesische Unternehmen Haier Biomedical genutzt. Das Unternehmen ist nach Kenntnis der Bundesregierung ein wichtiger Lieferant von Kühlaggregaten und Teil des CCEOP-Programms der Gavi. Ob die Angriffe erfolgreich waren, ist der Bundesregierung nicht bekannt. Die betroffenen Firmen sind dem genannten IBM-Bericht nach informiert. Dieser Bericht kann nach Auffassung der Bundesregierung jedoch technisch nicht zwingend untermauern, dass es sich um isolierte, herausgehobene Angriffe auf die Impfstoffversorgung handelt und nicht um Begleiterscheinungen der ubiquitären Bedrohung durch Ransomware für jedes an das Internet angeschlossene Netzwerk.

Zudem hat das für temperaturgesteuerte Lieferketten in der Lebensmittelbranche bekannte Logistikunternehmen Americold bestätigt, dass es Opfer eines Cyber-Angriffes geworden ist. Der Ransomware-Angriff habe sich bereits am 16. November 2020 ereignet und die folgenden Systeme beeinträchtigt: Telefonanlage, E-Mailverkehr, Bestands- und Bestellverwaltung. Medienberichten

zufolge soll das Unternehmen Gespräche geführt haben, um die Lagerung und Lieferung des COVID-19-Impfstoffes zu übernehmen.

Wie alle Einrichtungen, die IT nutzen, besteht auch für die in der Fragestellung genannten Einrichtungen die Gefahr von ungezielten Angriffen wie beispielsweise Ransomware.

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)?

Die Warnungen beruhten auf Berichten von Sicherheitsunternehmen sowie Warnungen von Partnerbehörden des BSI aus dem Ausland über Spionageangriffe auf Impfstoffhersteller durch Gruppen wie Kimsuky und die Schadsoftware WellMess.

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)?

Die Bundesregierung verweist auf ihre Antwort zu Frage 15. Anlässlich der Veröffentlichung des deutsch-französischen Lagebildes der Cyber-Sicherheit am 17. Dezember 2020 hat das BSI auf die Gefährdungslage im Gesundheitsbereich hingewiesen (https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2020/DF-Lagebild_171220.html).

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)?

Die Sicherheitsbehörden des Bundes stehen über das Nationale Cyber-Abwehrzentrum mit Unternehmen in Kontakt, die an der Impfstoff-Entwicklung, -Produktion und -Lieferung beteiligt sind.

Darüber hinaus hat das BfV im Rahmen der Präventionsarbeit und entsprechend seiner Erkenntnislage alle Impfstoffhersteller und an diesem Prozess beteiligte Akteure in Hinblick auf mögliche Sicherheitsrisiken sensibilisiert. Dies erfolgte bezogen auf die bekannten großen Akteure in persönlichen Gesprächen bzw. per Videokonferenz. In einem weiteren Rahmen wurden aber jeweils auch die betroffenen Branchen schriftlich sensibilisiert und die Ansprechbarkeit des BfV angezeigt. Diese Sensibilisierungsschreiben werden branchenspezifisch über funktionsfähige Kommunikationskanäle meistens von Fachverbänden vermittelt.

Im Übrigen wird auf die Antwort zu Frage 11 verwiesen.

Die Bundesregierung ist nach sorgfältiger Abwägung zu der Auffassung gelangt, dass eine weitergehende Beantwortung der Frage nicht offen erfolgen kann. Gegenstand der Frage sind solche Informationen, die in besonderem Maße das Staatswohl berühren. Die Einstufung als Verschlusssache ist erforderlich, weil die konkrete öffentliche Nennung der Beratungstermine der einzelnen Impfstoffhersteller sich negativ auf deren Bereitschaft zu zukünftigen Beratungen auswirken und damit nachteilig für die Interessen der Bundesrepublik Deutschland sein könnte.

Die Bundesregierung verweist für weitergehende Informationen insofern auf die als „VS – Nur für den Dienstgebrauch“ eingestufte Anlage.*

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.)?

Das BSI hat mit Unterstützung der zuständigen Gesundheitsbehörden, den Sicherheitsbehörden des Bundes und Branchenverbänden im Gesundheitswesen im Kontext SARS-CoV-2/COVID-19 wichtige Unternehmen identifiziert und steht auch international im Austausch mit Behörden anderer Länder.

Des Weiteren stehen das BSI und die Sicherheitsbehörden des Bundes über das Nationale Cyber-Abwehrzentrum mit Unternehmen in Kontakt, die an der Impfstoff-Entwicklung, -Produktion und -Lieferung beteiligt sind. Dort wurde eine entsprechende Arbeitsgruppe eingerichtet. In Zusammenarbeit mit den betroffenen Unternehmen wurde und wird die Lieferkette zur Verteilung und Produktion der Impfstoffe analysiert. Sowohl die dynamische Lage als auch die komplexe Lieferkette lassen eine Abschätzung zum Abschluss des Prozesses noch nicht zu.

Darüber hinaus hat das BKA am 24. November 2020 eine Gefährdungsbewertung für den Phänomenbereich der Politisch motivierten Kriminalität im Zusammenhang mit der Produktion, Lagerung und dem Transport von COVID-19 Impfstoffen sowie der Einrichtung von Impfzentren über verschiedene Wirtschaftsverbände der Wirtschaft allgemein zur Verfügung gestellt.

Zudem analysiert das BfV laufend die potentiell gefährdeten Prozesse im Hinblick auf die Fragestellung, welche Akteure mit welchen Informationen versorgt werden müssen. Dabei setzt das BfV zum einen auf die Expertise von Brancheninsidern wie z. B. Fachverbände oder spezifische Arbeitsgruppen, andererseits kann es über die Landesbehörden für Verfassungsschutz auf eine oft bereits über Jahre bestehende Vor-Ort-Expertise der dortigen Bereiche zurückgreifen.

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

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.)?

Die Antwort der Bundesregierung bezog sich auf konkrete Angriffe in Deutschland. Das BSI hat jedoch vor einer abstrakten Bedrohung gewarnt, nämlich potentieller Angriffe.

Somit besteht nach Auffassung der Bundesregierung kein Widerspruch zwischen der in der Frage genannten Antwort der Bundesregierung und den Mitteilungen des BSI. Auch wertet das BSI Angriffe mit Standard-Schadprogrammen wie zum Beispiel der auf Miltenyi Biotec (vgl. Antwort zu Frage 2) nicht als einen gezielten Angriff auf „Corona-Impfstoffhersteller und Versorgungsketten“.

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?

Das BSI hat erstmalig am 9. Dezember 2020 15:46 Uhr Kenntnis von einem Vorfall bei der EMA erhalten. Informationen, die über die Pressemittelung der EMA hinausgingen, lagen dem BSI am 10. Dezember 2020 vor.

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?

Die Bundesregierung teilt die Einschätzung der Fragestellerinnen und Fragesteller nicht. Sie hat die in der Frage genannte Schriftliche Frage mit dem damaligen Kenntnisstand beantwortet. Dort wurden Corona-Impfstoffherstellerinnen und -hersteller sowie Versorgungsketten (mitsamt Lagerung, Lieferung und Kühlung)“ adressiert; die EMA hingegen ist eine EU-Agentur.

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)?

Der Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit Informationstechnischer Systeme (IT-SiG 2.0) richtet sich nicht vorrangig an die den

COVID-19-Impfstoff herstellenden Unternehmen oder die in der Errichtung befindlichen Impfzentren. Durch die Klarstellung in § 5b BSIG-E haben die Impfzentren jedoch nun die Möglichkeit, im Notfall Unterstützung durch ein BSI-MIRT (Mobile Incident Response Team des BSI) anzufordern. Bereits jetzt fallen zudem einige Hersteller oder Distributoren unter die bestehende Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV), und es ist zu erwarten, dass andere Unternehmen aufgrund der höheren Impfstoffproduktion die Schwellenwerte 2021 erreichen und damit nach der bestehenden Systematik ab 2022 unter die BSI-KritisV fallen werden (die derzeit unter die BSI-KritisV fallenden Anlagen im Sektor Gesundheit sind einsehbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/it-digitalpolitik/bsi-kritisverordnung-poster.pdf?__blob=publicationFile&v=3).

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

Der Bundesregierung liegen keine Informationen über die konkret entwendeten Daten vor.

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?

Auf die Antwort zu Frage 23 wird verwiesen. Eine Abschätzung der möglichen Gefährdungslage ist ohne nähere Kenntnis der Art und des Umfangs der entwendeten Daten nicht möglich.

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?

Nach Erkenntnissen der Bundesregierung handelte es sich bei dem Angriff um einen Data-Breach mittels kompromittierter Zugangsdaten. Weitere Informationen im Sinne der Fragestellung liegen der Bundesregierung nicht vor.

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?

Der Bundesregierung liegen derzeit über keine Erkenntnisse vor, die den Schluss zuließen, dass es sich bei dem Angreifer um einen staatlichen Akteur gehandelt hat.

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

Der Vorfall ist den zuständigen Behörden des Bundes am 9. Dezember 2020 zur Kenntnis gelangt (vgl. Antwort zu Frage 20).

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)?

Das BSI hat, nachdem es am 9. Dezember 2020 über den Vorfall informiert wurde, mögliche Betroffene in Deutschland innerhalb von 24 Stunden informiert.

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?

Das BSI hat die möglichen betroffenen Unternehmen am 10. Dezember 2020 informiert. Ziel war es, die Unternehmen in die Lage zu versetzen, ähnliche Angriffe auf die eigenen Systeme detektieren und abwehren zu können sowie Informationen auszutauschen und die Bedrohungslage neu zu bewerten.

Das BKA hat Rückfrage bei BioNtech gehalten, ob dort nähere Erkenntnisse zum Vorfall und den ggf. ausgespähten Daten vorliegen. Die Anfrage blieb bis dato unbeantwortet.

Die Bundesregierung ist nach sorgfältiger Abwägung zu der Auffassung gelangt, dass eine weitergehende Beantwortung der Frage nicht offen erfolgen kann. Gegenstand der Frage sind solche Informationen, die in besonderem Maße das Staatswohl berühren. Die Einstufung als Verschlusssache ist erforderlich, da die Antwort Informationen enthalten, die im Zusammenhang mit der Arbeitsweise des Bundesamts für Verfassungsschutz stehen sowie Rückschlüsse auf dessen Erkenntnislage ermöglichen und hierdurch die weitere Aufklärung nachrichtendienstlicher Aktivitäten erheblich erschweren würde.

Die Bundesregierung verweist für weitergehende Informationen insofern auf die als „VS – Nur für den Dienstgebrauch“ eingestufte Anlage.*

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

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

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?

Der Bundesregierung liegen zu den genannten Angriffen keine eigenen, über die Medienberichterstattung hinausgehende Erkenntnisse vor.

Das BSI steht mit der US-Behörde für Cyber- und Infrastruktursicherheit im Austausch und wertet die Informationen über Angriffstechniken und verwendete Schadprogramme aus, um die eigenen Regierungsnetze zu schützen und Warnungen bzw. Handlungsempfehlungen an Unternehmen und Behörden zu verteilen.

Im Rahmen ihrer gesetzlichen Aufträge tauschen sich auch die Sicherheitsbehörden des Bundes mit den zuständigen US-Behörden zu Vorfällen, wie sie in der Fragestellung genannt sind, aus.

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