Deutscher Bundestag **Drucksache 20/10907**

20. Wahlperiode 02.04.2024

Antwort

der Bundesregierung

auf die Kleine Anfrage der Fraktion der CDU/CSU
– Drucksache 20/10657 –

Cyberattacken auf Krankenhäuser – Sachstand und Handlungsbedarf

Vorbemerkung der Fragesteller

Medienberichten zufolge steigen die Zahlen von Cyberattacken auf Krankenhäuser und Pflegeeinrichtungen seit den letzten Jahren deutlich an. Die Konsequenzen dieser Cyberattacken sind nicht nur hohe wirtschaftliche Schäden, sondern können auch Leben kosten (vgl. www.welt.de/wirtschaft/article246400880/Krankenhaeuser-Hacker-Angriffe-nehmen-zu-obwohl-sie-Leben-kosten.html). So wurden u. a. zuletzt zu Beginn des Jahres 2024 drei Krankenhäuser im Landkreis Soest in Nordrhein-Westfalen angegriffen, was u. a. dazu führte, dass die Rettungsleitstelle über längere Zeit Krankentransportwagen umleiten musste, die normalerweise zu den betroffenen Krankenhäusern gefahren wären (siehe www1.wdr.de/nachrichten/westfalen-lippe/hacker-angriff-hospital-lippstadt-100.html).

Mittlerweile ist die Bedrohungslage nach Einschätzung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) so hoch wie noch nie (vgl. www.swr.de/swraktuell/baden-wuerttemberg/heilbronn/immer-mehr-hackerangriffe-auf-kliniken-100.html). Im digitalen Zeitalter vermehren sich die Schnittstellen und Datenverbindungen zwischen den Krankenhäusern und dem Internet kontinuierlich. Mit immer mehr Digitalisierungsprojekten sind u. a. auch oft damit einhergehende Öffnungen der Kliniknetze verbunden, zudem werden entsprechende Schnittstellen geschaffen. Cyberattacken führen zu teils erheblichen wirtschaftlichen Schäden von Krankenhäusern und bedrohen die Versorgungsangebote sowie die vertraulichen Daten der Patientinnen und Patienten (vgl. www.aerzteblatt.de/nachrichten/149074/Krankenhaeuser-in-Sorge-wegen-Cyberangriffen). Die Angriffe sind zudem eine zusätzliche Belastung für die Krankenhäuser, die wegen des bekannten Fachkräftemangels und der drohenden Insolvenzwelle bereits mit anderen Problemen zu kämpfen haben. Gerade für kleinere Krankenhäuser ist der digitale Schutz häufig mit unverhältnismäßig hohen Kosten und einem hohen Aufwand verbunden. Darum sind Cyberattacken auf kritische Infrastrukturen wie Krankenhäuser nach Auffassung der Fragesteller dringend zu bekämpfen und zeigen akuten politischen Handlungsbedarf.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums für Gesundheit vom 28. März 2024 übermittelt.

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

1. Was ist der Bundesregierung insgesamt zu dieser Thematik bekannt?

Für die Bundesregierung ist die Sicherheit der Daten von Patientinnen und Patienten, aber auch die Verfügbarkeit einer qualitativ hochwertigen Gesundheitsversorgung ein essentielles Anliegen. Daher wurden durch den Bund eine Vielzahl regulatorischer (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik – BSIG; Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz – BSI-KritisV; § 75c des Fünften Buches Sozialgesetzbuch – SGB V) und praktischer Maßnahmen (Awareness-Maßnahmen, IT-Sicherheitsberatung, Forschungsvorhaben zur IT-Sicherheit in Krankenhäusern und zur Krankenhaus-IT) ergriffen, die zur Steigerung der IT-Sicherheit in der stationären Gesundheitsversorgung beitragen.

Mit seinem Bericht zur Lage der IT-Sicherheit in Deutschland gibt das Bundesamt für Sicherheit in der Informationstechnik (BSI) jährlich einen umfassenden Überblick über die Bedrohungen im Cyberraum. Wie dem Lagebericht 2023 zu entnehmen ist, ist derzeit die allgemeine Cyberbedrohungslage hoch. Die verschiedenen Tätergruppierungen unterscheiden bei ihren Angriffszielen nicht zwischen Akteuren der Wirtschaft und den Akteuren des Gesundheitssystems. Entsprechend der großen Bedeutung der Cybersicherheit im Sektor Gesundheit hat die Bundesregierung bereits 2018 in der BSI-KritisV Krankenhäuser besonders in den Blick genommen: Bei mehr als 30.000 vollstationären Fällen pro Jahr gilt ein Krankenhaus als kritische Anlage nach dem BSIG. Die mit dieser Einstufung verbundene Umsetzung des „Stands der Technik“ durch die regulierten KRITIS-Betreiber und die zahlreichen Hilfsangebote und Unterstützungsangebote durch das BSI sowie zusätzliche finanzielle Unterstützung durch das Bundesministerium für Gesundheit (BMG) (siehe auch Antwort zu den Fragen 15 und 16 bezüglich der Förderung im Rahmen des Krankenhauszukunftsfonds) haben zu einer Verbesserung der Situation beigetragen (siehe zurückgehende Vorfallzahlen in der Antwort zu Frage 3).

Mit der Einführung des § 75c SGB V durch das Patientendaten-Schutz-Gesetz vom 14. Oktober 2020 wurden zudem auch ab dem 1. Januar 2022 alle Krankenhäuser unterhalb der KRITIS-Schwelle zur Einhaltung dem Stand der Technik angemessener Vorkehrungen zur Verbesserung der Cybersicherheit verpflichtet, sodass seither ein Mindestsicherheitsniveau für alle Krankenhäuser in Deutschland besteht.

Die Krankenhäuser wurden bei der Umsetzung dieser Anforderungen unter anderem durch einen eigenen Fördertatbestand im Krankenhauszukunftsfonds (vgl. Antwort zu den Fragen 15 und 16) unterstützt.

Erst jüngst wurden die Regelungen für Krankenhäuser unter der KRITIS-Schwelle mit dem Digital-Gesetz um den wichtigen Aspekt der zu steigernden Security-Awareness von Mitarbeiterinnen und Mitarbeiter (Regelungsstandort nunmehr § 391 SGB V) verschärft.

2. Welche verschiedenen Gefahren durch Cyberattacken sind der Bundesregierung bekannt?

Cyberattacken zielen auf die Grundwerte der IT-Sicherheit: Vertraulichkeit, Integrität und Verfügbarkeit. Üblicherweise wird durch Verschlüsselung von Daten durch Ransomware die Arbeitsfähigkeit von Krankenhäusern gestört und durch die Exfiltration von Daten die Vertraulichkeit von Patientendaten kompromittiert.

Darüber hinaus hat das BSI zu den verschiedenen Gefahren durch Cyberattacken ausführlich in seinem Jahresbericht 2023 Teil B: „Erkenntnisse zur Gefährdungslage in der Gesellschaft“ berichtet www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html.

3. Wie viele Fälle solcher Cyberattacken auf deutsche Krankenhäuser (inklusive Bundeswehrkrankenhäuser) sind der Bundesregierung bekannt (bitte nach Jahren seit 2010 bis 2024 sowie nach [Betten-]Größe der betroffenen Krankenhäuser aufschlüsseln)?

Für KRITIS-Betreiber gilt die Meldepflicht für Cybersicherheitsvorfälle gemäß § 8b Absatz 4 BSIG. Aus den eingegangenen Meldungen lässt sich pro Branche und KRITIS-Sektor eine Meldestatistik exportieren. Die folgenden Zahlen gelten dabei nur für Krankenhäuser, die unter die BSI-KritisV fallen (Bundeswehrkrankenhäuser fallen derzeit nicht unter die BSI-KritisV). Die Bettenzahl pro Krankenhaus wird nicht erfasst, da für die Identifikation von KRITIS-Betreibern nur die vollstationären Fälle pro Jahr ausschlaggebend sind (siehe BSI-KritisV). Da die Umsetzung des § 8a BSIG für den Sektor Gesundheit erst bis spätestens 30. Juni 2019 erfolgen musste, beinhaltet die Statistik nur Pflichtmeldungen ab 2018, die von KRITIS-Krankenhäusern abgegeben wurden. Erfasst wurden nur Vorfälle, bei denen es sich um „informationstechnische Angriffe“ handelte:

- 2018 – 17 Vorfälle,
- 2019 – 61 Vorfälle,
- 2020 – 55 Vorfälle,
- 2021 – 35 Vorfälle,
- 2022 – 35 Vorfälle,
- 2023 – 21 Vorfälle,
- 2024 – drei Vorfälle (bisher im Zeitraum 1. Januar 2024 bis 18. März 2024).

Für Krankenhäuser, die nicht unter die BSI-KritisV fallen, bestehen keine bundesrechtlichen Meldepflichten einer Cyberattacke.

4. Erkennt die Bundesregierung Muster bei der Zielgruppe der angegriffenen Krankenhäuser, und wenn ja, welche?

Das BSI erfasst laut gesetzlichem Auftrag nach dem BSIG IT-Störungen bei KRITIS-Betreibern, deswegen können keine gesamtheitlichen Muster erkannt werden, die über diesen Bereich hinausgehen.

5. Erhebt die Bundesregierung Informationen darüber, auf welche Weise die Cyberattacken durchgeführt werden, wenn ja, auf welche Weise werden die Krankenhäuser angegriffen, und wenn nein, wieso nicht?

Hierzu werden keine Informationen durch das BSI erhoben, da dies nicht dem gesetzlichen Auftrag nach BSIG entspricht. Im Übrigen wird auf die Antwort zu Frage 2 verwiesen.

6. Mit welchen Krankenhausverbänden und wann hat die Bundesregierung ihre bisherigen Gesetzesvorhaben bezüglich des Schutzes der Krankenhäuser vor Cyberattacken abgestimmt?

Für den Bereich der KRITIS-Regulierung wurden im Rahmen der Verbändeanhörung zur 1. Änderungsverordnung der BSI-KritisV im Jahr 2017 die Deutsche Krankenhausgesellschaft und der Verband der Universitätsklinika Deutschlands angehört.

Mit Blick auf die Regulierung der Cybersicherheit der Krankenhäuser im Fünften Buch Sozialgesetzbuch (§ 75c alte Fassung beziehungsweise § 391 neue Fassung) wurden im Rahmen des Patientendaten-Schutz-Gesetzes im Jahr 2020 die Deutsche Krankenhausgesellschaft und der Verband der Universitätsklinika Deutschlands angehört und im Jahr 2023 im Rahmen des Digital-Gesetzes die Deutsche Krankenhausgesellschaft, der Verband der Universitätsklinika Deutschlands und der Bundesverband der Krankenhaus IT-Leiterinnen/Leiter.

7. Wie hoch sind nach Kenntnissen der Bundesregierung die wirtschaftlichen Schäden für die betroffenen Krankenhäuser?

Darüber liegen der Bundesregierung keine Erkenntnisse vor.

8. Welche Auswirkungen haben Cyberangriffe nach Ansicht der Bundesregierung auf die Verlässlichkeit der Patientenversorgung?

Allgemein gilt: Erfolgreiche Cyberangriffe können sich negativ auf die Grundwerte der IT-Sicherheit auswirken, also die Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und der mit ihnen verarbeiteten Daten beeinträchtigen. Sofern IT-Systeme im Gesundheitswesen eingesetzt werden, sind daher organisatorische und technische Vorkehrungen durch die Krankenhäuser zu ergreifen, die gerade die Folgen eines Ausfalls oder Beeinträchtigung des Krankenhausbetriebs verhindern sollen und zudem den besonderen Schutzbedarf der verarbeiteten Patienteninformationen in den Blick nehmen. Daher sind beispielsweise im Branchenspezifischen Sicherheitsstandard „Medizinische Versorgung“ für die Krankenhäuser bereits Aspekte zum Betrieblichen Kontinuitätsmanagement (business continuity management) enthalten.

9. Erhebt die Bundesregierung regelmäßig Informationen dazu, welche Auswirkungen Cyberangriffe auf die Arbeitsweise der Ärztinnen und Ärzte und Mitarbeiterinnen und Mitarbeiter im Krankenhaus haben, wenn ja, was hat die Bundesregierung dabei festgestellt, und wenn nein, warum nicht?

Es besteht keine bundesgesetzliche Kompetenz zur Erfassung von Daten im Sinne der Fragestellung, sodass der Bundesregierung hierzu keine Erkenntnisse vorliegen.

10. Wie lange fällt nach Kenntnissen der Bundesregierung ein Krankenhaus durchschnittlich pro Cyberattacke für die Versorgung von Patientinnen und Patienten aus?

Es besteht keine bundesgesetzliche Kompetenz zur Erfassung von Daten im Sinne der Fragestellung, sodass der Bundesregierung hierzu keine Erkenntnisse vorliegen.

11. Was sind aus Sicht der Bundesregierung die Ursachen dafür, dass es vermehrt zu solchen Cyberattacken auf Krankenhäuser kommt?

Wie in der Antwort zu Frage 1 ausgeführt, ist nicht erkennbar, dass die Angreifer zwischen Krankenhäusern und anderen Wirtschaftsbeteiligten differenzieren, so dass eine Motivation zu einer Fokussierung auf Krankenhäuser nicht erkennbar ist. Im Übrigen ist die Anzahl der gemeldeten IT-Sicherheitsvorfälle bei KRITIS-Krankenhäusern seit dem Jahr 2019 rückläufig.

12. Welche Informationen liegen der Bundesregierung über den Hintergrund der entsprechenden Tätergruppierungen vor?

13. Welche Informationen hat die Bundesregierung darüber, welche Rolle bei den Cyberattacken ausländische Nachrichtendienste spielen, die die kritische Infrastruktur in Deutschland destabilisieren wollen?

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

Zu den Fragestellungen liegen der Bundesregierung keine Erkenntnisse vor.

14. Plant die Bundesregierung eine Verschärfung strafrechtlicher Maßnahmen gegen die Täter von Cyberattacken z. B. auf Krankenhäuser, wenn ja, welche, und wenn nein, warum nicht?

Zur Prüfung der Frage, ob die Tatbestände und Strafrahmen der §§ 202a ff., §§ 303a f. des Strafgesetzbuchs den aktuellen Entwicklungen ausreichend gerecht werden und ob die zu einer effektiven Verfolgung erforderlichen Ermittlungsinstrumente zur Verfügung stehen sowie zur Klärung der Frage, wie das Identifizieren und Melden von Sicherheitslücken in der IT-Sicherheitsforschung, ohne Strafbarkeitsrisiken ermöglicht werden kann, hat das Bundesministerium der Justiz zwei Symposien (am 30. Juni und am 4. Oktober 2023) durchgeführt. Das Ergebnis wird derzeit ausgewertet.

15. Plant die Bundesregierung, für die IT-Sicherheit der Krankenhäuser gesonderte Fördermittel des Bundes bereitzustellen, insbesondere vor dem Hintergrund der aktuellen Finanzprobleme der Krankenhäuser, und wenn nein, warum nicht?

16. Wie bewertet die Bundesregierung die Idee eines Krankenhauszukunftsgesetzes II, im Rahmen dessen die Sicherung der digitalen Infrastruktur von Krankenhäusern gestärkt werden könnte?

Die Fragen 15 und 16 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Im Rahmen der dualistischen Krankenhausfinanzierung ist es Aufgabe der Länder, Investitionsvorhaben der Krankenhäuser zu fördern. Dies gilt auch für Investitionsvorhaben zur Verbesserung der digitalen Ausstattung der Krankenhäuser. Dennoch hat der Bund mit dem Krankenhauszukunftsgesetz (KHZG), das am 29. Oktober 2020 in Kraft getreten ist, ein „Zukunftsprogramm Krankenhäuser“ aufgelegt, um die Digitalisierung von Krankenhäusern zu fördern. Es wurden 3 Mrd. Euro aus Bundesmitteln in einen Krankenhauszukunftsfonds eingestellt. Zusammen mit der erforderlichen Kofinanzierung aus Mitteln der Länder oder der Krankenhausträger in Höhe von 30 Prozent standen damit insgesamt 4,3 Mrd. Euro zur Verfügung, um durch gezielte Projekte das Digitali-

sierungsniveau erheblich anzuheben. Zahlreiche Projekte befinden sich derzeit in der Umsetzung.

Der mit der Förderung aus dem Krankenhauszukunftsfonds erreichte Reifegrad der Krankenhäuser hinsichtlich der Digitalisierung wird derzeit evaluiert. Diese Auswertung wird zu berücksichtigen sein bei der Frage, inwieweit der Bund eine weitere Unterstützung der Länder bei der Förderung von digitalen Investitionsvorhaben in Krankenhäusern leisten kann und sollte.

17. Wie will die Bundesregierung konkret dafür sorgen, dass die Zahlen solcher Cyberattacken wieder signifikant zurückgehen oder zumindest nicht weiter ansteigen?

In Bezug auf die Unterstützung von KRITIS-Betreibern liegt der Fokus auf der Absicherung der potentiellen Opfer, die sich auch aus der Regulierung ergibt. Hier sieht sich die Bundesregierung beim Schutz von KRITIS durch die Anzahl der gemeldeten Vorfälle auf einem guten Weg. Auf Basis der Befugnisse aus dem BSIG müssen Betreiber kritischer Infrastrukturen Nachweise über die Absicherung nach dem Stand der Technik erbringen und die im Rahmen der regelmäßigen Auditierung erkannten Lücken schließen. Das BSI nutzt dabei die zur Verfügung stehenden Regulierungsinstrumente um die KRITIS-Betreiber bei der Verbesserung ihrer IT-Sicherheit zu unterstützen, um potentielle Angriffsversuche zu unterbinden, zu erkennen und abzuwehren. Angreifer können aber nicht von Angriffsversuchen abgehalten werden.

Mit Blick auf die Krankenhäuser unterhalb der KRITIS-Schwelle wurden die bestehenden Regelungen durch das Digital-Gesetz jüngst verschärft.

18. Welche Programme unterstützt die Bundesregierung zur Prävention solcher Cyberattacken auf kritische Infrastrukturen im Allgemeinen, und welche Maßnahmen plant die Bundesregierung konkret, um die Krankenhäuser bei dem Umgang mit diesen Attacken zu unterstützen?

Neben Sensibilisierungsvorträgen, regelmäßigem Austausch innerhalb der Branchenarbeitskreise und direkt mit den KRITIS-Betreibern, unterstützt das BSI Branchenverbände bei der Erstellung sogenannter „Branchenspezifischer Sicherheitsstandards“ (B3S). Ein von einem Branchenverband erstellter B3S wird durch das BSI auf dessen Eignung geprüft und im Falle eines positiven Ergebnisses eignungsfestgestellt. Hierbei werden branchenspezifische Vorgaben zum Stand der Technik und konkrete Maßnahmen zur Absicherung und Verbesserung der IT-Sicherheit formuliert. Der aktuell gültige B3S „Medizinische Versorgung“ richtet sich bzgl. der Zielgruppe nicht nur an KRITIS-Betreiber, sondern allgemein an alle Krankenhäuser, da dessen Nutzung auch als favorisierte Umsetzungsvariante der Vorgaben des § 75c SGB V (beziehungsweise § 391 SGB V n. F.) vorgesehen ist.

19. Könnte die geplante Krankenhausreform nach Ansicht der Bundesregierung die Situation weiter verschärfen, wenn ja, was gedenkt die Bundesregierung, zum Schutz der Krankenhäuser im Rahmen des entsprechenden Gesetzgebungsverfahrens zu unternehmen, und wenn nein, warum nicht?

20. Erwartet die Bundesregierung, dass die Krankenhausreform zu gezielteren Cyberangriffen auf die Maximalversorgungskrankenhäuser führt, wenn ja, wie möchte die Bundesregierung diese Maximalversorgungskrankenhäuser besonders schützen, und wenn nein, warum nicht?

Die Fragen 19 und 20 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Die Regelungsinhalte der geplanten Krankenhausreform betreffen nicht die IT-Sicherheit der Krankenhäuser.

21. Wie verhält sich die Bundesregierung zu aktuellen Diskussionen zu einer Verordnung für mehr Cybersicherheit auf EU-Ebene, ist nach Ansicht der Bundesregierung mit einer Verabschiedung der Verordnung vor der Europawahl zu rechnen, und wie plant die Bundesregierung, diese Verordnung konkret umzusetzen?

Aus der Fragestellung ist nicht klar erkennbar, welche der EU-Verordnungen gemeint ist. Auf EU-Ebene werden derzeit verschiedene Verordnungen zum Themenkreis der Cybersicherheit diskutiert. Für den Cyber Resilience Act (Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020) gilt, dass am 12. März 2024 das Europäische Parlament diesen in erster Lesung angenommen hat. Damit ist nur noch die Annahme des Rates ausstehend. Nach Ansicht der Bundesregierung ist mit einer Annahme vor der Neuwahl des Europäischen Parlaments zu rechnen. Da es sich um eine Verordnung handelt, wird diese unmittelbar nach ihrem Inkrafttreten in Deutschland gelten.

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