Deutscher Bundestag **Drucksache 19/19392**

19. Wahlperiode 22.05.2020

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Jan Nolte, Gerold Otten, Jens Kestner, weiterer Abgeordneter und der Fraktion der AfD
– Drucksache 19/18797 –

Cyber-Angriffe auf medizinische Einrichtungen und Geräte

Vorbemerkung der Fragesteller

Laut einer Studie der Unternehmensberatung Roland Berger aus dem Jahr 2017 wurden mindestens 64 Prozent aller deutschen Krankenhäuser mindestens schon einmal Ziel von Cyber-Attacken (vgl. Roland Berger: Krankenhaus-Studie 2017, München 2017). Die Angriffe können unspezifiziert, zum Beispiel durch zufällig eingeschleuste Malware erfolgen oder gezielt, zum Beispiel für den Diebstahl von Patientenakten oder für die Manipulation medizinischer Geräte durchgeführt werden (ebd.).

1. Welche staatliche Kontrolle und Evaluation wird zur Cyber-Sicherheit von Krankenhäusern sowie deren Geräten und Anlagen durchgeführt?

Krankenhäuser in Deutschland, die den Schwellenwert von 30.000 vollstationären Fällen pro Jahr gemäß BSI-KRITIS-Verordnung (BSI-KritisV) erreichen, sind über das BSI-Gesetz (BSIG) reguliert und müssen sich beim Bundesamt für Sicherheit in der Informationstechnik (BSI) als Betreiber Kritischer Infrastrukturen registrieren lassen. Sie sind damit verpflichtet, angemessene Sicherheitsmaßnahmen zum Schutz ihrer IT-Systeme, Komponenten und Prozesse nach Stand der Technik umzusetzen. Dies müssen sie nach § 8a Absatz 3 BSIG alle zwei Jahre gegenüber dem BSI nachweisen.

2. Welche nationalen und internationalen Cyber-Security-Zertifikate werden für medizinische Geräte vergeben?

Es gibt nach Kenntnisstand der Bundesregierung weder nationale noch internationale spezielle Cyber-Sicherheitszertifikate für medizinische Geräte. Es gibt nationale und internationale Empfehlungen zur Cyber-Sicherheit von Medizinprodukten (BSI, FDA, MDCG, IMDRF).

Grundsätzlich dürfen Medizinprodukte nur mit einer CE-Kennzeichnung in Verkehr gebracht oder in Betrieb genommen werden. Mit einer CE-Kennzeichnung weist der Hersteller nach, dass sein Produkt die grundlegenden Anforde-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 22. Mai 2020 übermittelt.

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

rungen erfüllt, also sicher und entsprechend der medizinischen Zweckbestimmung medizinisch-technisch leistungsfähig ist, sowie ein vorgeschriebenes Konformitätsbewertungsverfahren durchgeführt hat.

Art und Umfang der Beteiligung einer unabhängigen Zertifizierungsstelle (Benannten Stelle) am Konformitätsbewertungsverfahren hängt vom potentiellen Risiko des Produktes ab. Die Ausgestaltung der Konformitätsbewertungsverfahren und deren Durchführung in Deutschland sind in der Verordnung über Medizinprodukte (MPV) geregelt, die auf entsprechende europäische Richtlinien verweist.

3. Wie häufig wurden nach Kenntnis der Bundesregierung im Jahre 2019 Krankenhäuser Ziel von Cyber-Attacken?

Das BSI erfasst im Auftrag der Bundesregierung IT-Sicherheitsvorfälle, zu denen unter anderem Cyber-Angriffe zählen, als zentrale Meldestelle für die IT-Sicherheit Kritischer Infrastrukturen nach § 8b BSIG. Seit Inkrafttreten der ersten Änderungsverordnung der BSI-KritisV am 30. Juni 2017 gilt diese Meldepflicht auch für den Sektor Gesundheit. Einrichtungen aus diesem Sektor, die nach § 6 BSI-KritisV als Kritische Infrastruktur gelten, sind hiernach zu Meldungen verpflichtet.

Im Rahmen dieser Meldepflicht liegen dem BSI für das Jahr 2019 insgesamt 14 Meldungen aus den Krankenhäusern zu Cyber-Angriffen vor.

a) Was waren nach Kenntnis der Bundesregierung die jeweiligen Auswirkungen?

Von der souveränen Abwehr (technisch am Perimeter oder durch aufmerksame IT-Nutzer), d. h. ohne Auswirkung auf die Kritische Infrastruktur bzw. die kritische Dienstleistung, bis hin zu mehrtägigen Ausfällen (über die dann auch hinlänglich durch die Presse berichtet wurde) sind alle Varianten vorzufinden. Mehrtägige Ausfälle sind jedoch dabei die Seltenheit.

b) Von welchem staatlichen oder nichtstaatlichen Akteur wurden nach Kenntnis der Bundesregierung die Angriffe jeweils aufgeklärt?

c) Welcher Täterkreis (kriminelle, staatliche Akteure usw.) konnte nach Kenntnis der Bundesregierung identifiziert werden?

Der Bundesregierung liegen zur Fragestellung keine Erkenntnisse vor.

4. Wie entwickelte sich nach Kenntnis der Bundesregierung die Anzahl der Angriffe auf medizinische Einrichtungen seit 2010 im Vergleich zum jeweiligen Vorjahr prozentual?

Die Meldepflicht für Anlagen die unter das BSIG fallen, besteht erst seit dem Jahr 2018. Es liegen folgende Zahlen vor:

- 2018: Stationäre med. Versorgung: 14; Versorgung mit Arzneimitteln: 1; Versorgung mit Medizinprodukten: 0; Laboratoriumsdiagnostik: 1
- 2019: Stationäre med. Versorgung: 14; Versorgung mit Arzneimittel: 1; Versorgung mit Medizinprodukte: 0¸ Laboratoriumsdiagnostik: 0

5. Insgesamt wie viele Krankenhäuser wurden nach Kenntnis der Bundesregierung bisher Ziel von Cyber-Angriffen?

Dem BSI wurden im Rahmen der gesetzlichen Meldepflicht seit dem Jahr 2018 bis heute von 27 Klinik-Betreibern Cyber-Angriffe mitgeteilt.

Die abweichende Zahl gegenüber Frage 4 ergibt sich aus der Tatsache, dass ein Betreiber zwei Meldungen nach BSIG abgegeben hat.

6. Welche medizinischen Geräte und Anlagen waren nach Kenntnis der Bundesregierung bisher Ziel von Cyber-Angriffen?

   a) Welcher Art waren die Angriffe?

   b) Welche Folgen hatten die Angriffe?

   c) Welche Maßnahmen wurden zur Sicherung dieser Geräte ergriffen?

Der Bundesregierung liegen zur Fragestellung keine Erkenntnisse vor.

7. Welche medizinischen Geräte und Anlagen sind nach Kenntnis der Bundesregierung potenziell gefährdet?

   Welche Gegenmaßnahmen sind von Seiten der Bundesregierung identifiziert oder durchgeführt worden?

Je mehr Kommunikationsschnittstellen ein Medizinprodukt aufweist, desto größer ist die potenzielle Angriffsoberfläche. Das BSI führt kontinuierliche Sicherheitsanalysen im Bereich moderner Medizinprodukte durch. Des Weiteren besteht eine vertrauensvolle Zusammenarbeit mit dem Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) bei der Behebung bekannt gewordener Schwachstellen in Medizinprodukten. Künftig plant das BSI einen Ausbau dieser Zusammenarbeit zur Etablierung einer Sicherheitszertifzierung.

8. Welche Manipulationen von patientenbezogenen Daten sind der Bundesregierung bekannt?

Der Bundesregierung liegen zur Fragestellung keine Erkenntnisse vor.

9. Welche Unterstützung erhielten medizinische Einrichtung von Seiten staatlicher Akteure für eine bessere Sicherung ihrer Informationstechnik (IT) und Gerätschaften?

Mit dem IT-Grundschutz des BSI oder den Empfehlungen, die das BSI im Rahmen der Allianz für Cyber-Sicherheit zur Verfügung gestellt hat, wurden den medizinischen Einrichtungen vielfältige Werkzeuge zur Absicherung ihrer IT-Infrastruktur zur Verfügung gestellt. Zudem hat die Deutsche Krankenhausgesellschaft einen branchenspezifischen Sicherheitsstandard („B3S“) erarbeitet, der allen Krankenhäusern zur Verfügung steht. Dieser B3S wurde durch das BSI geprüft und die Eignung für eine Einhaltung des Stands der Technik gem. § 8a (1) Satz 2 BSIG festgestellt. Daran können sich auch die Kliniken orientieren, die nicht unter die gesetzlichen Vorgaben fallen.

Es wird außerdem auf die Antwort zu Frage 10 verwiesen.

10. Wie hoch waren die finanziellen Zuwendungen des Bundes für die Cyber-Sicherheit medizinischer Einrichtungen in den Jahren 2017 bis 2019?

    Welche Zuwendungen sind für 2020 bis 2023 geplant?

Für die Förderung der Investitionskosten im Krankenhausbereich, unter anderem auch für die digitale (Sicherheits-)Infrastruktur, sind die Länder zuständig.

Über den fortgeführten Krankenhausstrukturfonds können die Länder seit 2019 bis Ende 2022 Mittel in Höhe von insgesamt bis zu 2 Mrd. Euro für strukturverbessernde Vorhaben im Krankenhausbereich aus der Liquiditätsreserve des Gesundheitsfonds erhalten. Mittel aus dem Krankenhausstrukturfonds können unter anderem für die Förderung von Vorhaben zur Anpassung der informationstechnischen Sicherheit von Krankenhäusern mit mindestens 30 000 vollstationären Behandlungsfällen pro Jahr an die Vorgaben des BSI-Gesetzes gewährt werden. Bislang wurden seitens der Länder noch keine Anträge gestellt, sodass der Bundesregierung bislang keine Erkenntnisse vorliegen darüber, für welche Fördervorhaben Mittel letztlich abfließen werden.

11. Wie hoch sind nach Kenntnis der Bundesregierung im Durchschnitt die veranschlagten Haushaltsmittel der medizinischen Einrichtungen für IT-Sicherheit?

Der Bundesregierung liegen zur Fragestellung keine Erkenntnisse vor. Die Mittelverwaltung und Finanzplanung liegt in der Zuständigkeit der Betreiber.

12. Welche staatlichen Maßnahmen sind in Zukunft für eine höhere Sicherheit der Krankenhäuser und medizinischen Geräte geplant?

Alle Kliniken sind angehalten, die bestehenden IT-Sicherheitsmaßnahmen nach dem Stand der Technik umzusetzen und sich dabei zum Beispiel am IT-Grundschutz des BSI, an dem branchenspezifischen Sicherheitsstandard (siehe § 8a Absatz 2 BSIG) der Deutschen Krankenhausgesellschaft oder an den Empfehlungen zu orientieren, die das BSI im Rahmen der Allianz für Cyber-Sicherheit zur Verfügung stellt. Diese Regelungen beschreiben ein umfassendes Sicherheitspaket und bedürfen zum jetzigen Zeitpunkt keiner Erweiterung.

13. Welche zukünftigen Herausforderungen und Gefahren hat die Bundesregierung in diesem Zusammenhang identifiziert?

Die Bedrohungslage für die Unternehmen wird zukünftig auch weiterhin bestehen. Die Bundesregierung wird den Themenkomplex weiter beobachten und geeignete Maßnahmen ergreifen.

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