Deutscher Bundestag **Drucksache 19/18208**

19. Wahlperiode 19.03.2020

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Dr. Wieland Schinnenburg, Michael Theurer, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 19/17505 –

Gewährleistung der Datenhoheit von Versicherten in der Telematikinfrastruktur

Vorbemerkung der Fragesteller

Nach Plänen des Bundesministers für Gesundheit Jens Spahn soll die Telematikinfrastruktur und die mit ihr verbundene elektronische Patientenakte schnell eingeführt werden. Er wolle dort „Geschwindigkeit reinbringen“ (https://www.welt.de/politik/deutschland/article204789542/Jens-Spahn-Die-groesste-Bewaehrungsprobe-des-Gesundheitsministers.html). Nach Auffassung der Fragesteller ist eine beschleunigte Digitalisierung des Gesundheitswesens dringend geboten, jedoch muss diese Digitalisierung mit Augenmaß erfolgen.

Allerdings ist die Sicherheitsarchitektur der Telematikinfrastruktur nach Auffassung der Fragesteller noch nicht ausgereift. Im Rahmen des Kongresses 36c3 im Dezember 2019 stellten Martin Tschirsich, Dr. med. Christian Brodowski und Dr. André Zilch Angriffsmöglichkeiten vor, die nicht einmal die digitale Infrastruktur selbst betreffen, sondern vielmehr die Authentifizierungs- und Bestellprozesse für Konnektoren und Zugangskarten. So gelang es ihnen, einen Konnektor zu bestellen, einen Institutionsausweis, einen Heilberufsausweis und auch von Seiten der Patienten eine elektronische Gesundheitskarte als unberechtigte Personen zu bestellen. Als Grund nannten sie die unzureichenden Prozesse der Anbieter, die aber in den Vorgaben der gematik GmbH richtig definiert seien (https://www.youtube.com/watch?v=q6l_B2fgJjM).

Weitere Schwachstellen wurden in der Zeitschrift „c’t“ (3/2020) aufgedeckt. Dort wird etwa aufgeführt, dass Praxen unsichere Dokumente in die elektronische Patientenakte laden könnten. Weiter wird kritisiert, dass die Software der T-Systems-Konnektoren teilweise veraltet ist. Die Ende November 2019 veröffentliche Firmware 1.5.3 weise etwa 291 bekannte Sicherheitslücken auf. Betroffen sei aber auch das Kartenterminal „Orga 6141 online“. Beim Konnektor KoCoBox wäre es wegen eines Verstoßes gegen Open-Source-Lizenzen nicht möglich festzustellen, welche Sicherheitslücken durch veraltete Komponenten hier auftreten könnten, allerdings bestünde auch hier eine große Gefahr.

Nach Auffassung der Fragesteller ist die Datenhoheit der Versicherten über ihre Gesundheitsdaten von zentraler Bedeutung. Dass der Schutz dieser Daten sehr einfach überwunden werden kann, dürfte das Vertrauen in die Digitalisierung des Gesundheitswesens nicht stärken. Diese ist aber notwendig, um die

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums für Gesundheit vom 17. März 2020 übermittelt.

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

Versorgung zu verbessern und auch um in der Forschung neue Wege gehen zu können.

Vorbemerkung der Bundesregierung

Mitglieder des Chaos Computer Clubs haben Schwachstellen in den Ausgabeprozessen für Heilberufsausweis, Praxisausweis und elektronischer Gesundheitskarte bei den Kartenherausgebern identifiziert. Zu keinem Zeitpunkt waren dabei medizinische Daten gefährdet. Die Gesellschaft für Telematik und die zuständigen Aufsichtsbehörden haben schnell und entschlossen reagiert und die Ausgabe der Arzt- und Praxisausweise temporär gestoppt. Die Ausgabeprozesse konnten in der Zwischenzeit wieder aufgenommen werden.

Die Bundesregierung hat keine Anhaltspunkte, dass die Sicherheit der Konnektoren oder Kartenlesegeräte gefährdet sein könnte.

Datenschutz und Datensicherheit haben für die Bundesregierung beim Aufbau der Telematikinfrastruktur oberste Priorität. Deshalb sind Schwachstellen, wie sie der Chaos Computer Club aufgedeckt hat, nicht akzeptabel.

1. In welcher Anzahl von Praxen ist die Telematikinfrastruktur eingeführt?

2. In welcher Anzahl von Praxen, Kliniken, Apotheken und weiteren Gesundheitseinrichtungen ist die Telematikinfrastruktur noch nicht eingeführt worden, und wann soll sie hier flächendeckend eingeführt werden?

Die Fragen 1 und 2 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Derzeit sind bundesweit zwischen 80 und 90 Prozent der niedergelassenen Ärztinnen und Ärzte, Zahnärztinnen und und Zahnärzte an die Telematikinfrastruktur angeschlossen. In einzelnen Bundesländern und bei den Zahnärztinnen und Zahnärzten sind es generell über 90 Prozent. Darunter fallen auch Praxen ohne direkten Patientenkontakt, z. B. Labore, die sich erst bis zum 30. Juni 2020 an die Telematikinfrastruktur anschließen müssen. Der Anschluss der Apotheken und Krankenhäuser ist schwerpunktmäßig im zweiten Halbjahr 2020 vorgesehen.

3. Welche Anzahl an Einrichtungen wurde nach Kenntnis der Bundesregierung wegen der Nichteinführung der Telematikinfrastruktur gemäß § 291 des Fünften Buches Sozialgesetzbuch (SGB V) mit Honorarkürzungen belegt, in welcher Höhe sind hier insgesamt Honorare gekürzt worden, und wem kamen diese eingesparten Mittel zugute, bzw. wofür wurden sie verwendet?

Die Anzahl der Einrichtungen, die sanktioniert wurden, ist der Bundesregierung nicht bekannt. Der Bundesregierung hat ferner keine Zuständigkeit für die Entscheidung über die Verwendung der durch Kürzung der vertragsärztlichen Vergütung nach § 291 Absatz 2b Satz 9 des Fünften Buches Sozialgesetzbuch (SGB V) einbehaltenen Mittel.

4. Welche Sicherheitsvorkehrungen wurden ergriffen, seitdem bekannt ist (vgl. Vorbemerkung der Fragesteller), dass Institutions- und Heilberufsausweise auch von unberechtigten Personen bestellt werden konnten?

   a) Wie wird sichergestellt, dass die bereits ausgegebenen Ausweise auch ausschließlich von berechtigten Personen genutzt werden?

Die Fragen 4 und 4a werden gemeinsam beantwortet.

Bei Ausweisen, bei denen die Ausgabe auf eine potentiell unsichere Art und Weise erfolgte, wurden die Angaben plausibilisiert und im Zweifelsfall die Zustellung beim Empfänger verifiziert.

   b) Welche Anzahl der Institutionsausweise wurden jeweils mit den unsicheren Verfahren Bankident und Vorab-Kammerident ausgegeben, welche jeweils mit den sicheren Verfahren Postident und Kammerident?

Es wurden keine Institutionsausweise auf Basis von Bankident oder Vorab-Kammerident ausgegeben.

   c) Welche Anzahl der Heilberufsausweise wurde jeweils mit den unsicheren Verfahren Bankident und Vorab-Kammerident ausgegeben, welche jeweils mit den sicheren Verfahren Postident und Kammerident?

Die genannten Verfahren waren nicht prinzipiell unsicher, sondern lediglich unter bestimmten Bedingungen angreifbar. Nach aktuellem Wissenstand wurden nahezu alle Heilberufsausweise mit Zugriffsmöglichkeit auf die elektronische Gesundheitskarte (insgesamt weniger als 1000) mittels des PostIdent-Verfahrens ausgegeben. Bei Vorgängerkarten des aktuellen Heilberufsausweises, ohne Zugriffsmöglichkeit auf die elektronische Gesundheitskarte und die Telematikinfrastruktur, wurde vornehmlich das Bankident-Verfahren verwendet.

   d) Plant die Bundesregierung, möglicherweise kompromittierte Ausweise neu auszugeben, wenn ja, wann, und in welchem Umfang?

Es wurden nur die aus den Medien bekannten und zu Demonstrationszwecken durchgeführten Fälle einer missbräuchlichen Kartenausgabe identifiziert, bei denen jeweils die Karteninhaberin bzw. der Karteninhaber sein Einverständnis gab.

   e) Welchen Einfluss haben die ergriffenen Maßnahmen auf die Honorarkürzungen gemäß § 291 SGB V?

Die Bundesregierung sieht keinen Bedarf für Anpassungen an den gesetzlichen Bestimmungen zu Honorarkürzungen gemäß § 291 Absatz 2b SGB V aufgrund der ergriffenen Maßnahmen.

5. Welche Sicherheitsvorkehrungen wurden ergriffen, um zu gewährleisten, dass die elektronische Gesundheitskarte nur an berechtigte Personen ausgegeben wird?

   a) Wie wird sichergestellt, dass Adressänderungen auch tatsächlich nur von berechtigten Personen veranlasst wurden?

   b) Welche Authentifizierungsverfahren sind zur Ausstellung einer elektronischen Gesundheitskarte zulässig, und wie wird überwacht, dass diese auch eingesetzt werden?

   c) Müssten bis zur Einführung der elektronischen Patientenakte nicht alle elektronischen Gesundheitskarten ausgetauscht und neu authentifiziert werden, damit sichergestellt ist, dass nur berechtigte Personen diese verwenden?

Die Fragen 5 bis 5c werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Der Spitzenverband Bund der Krankenkassen erhielt durch § 217f Absatz 4b SGB V den Auftrag, eine Richtlinie zum Schutz von Sozialdaten der Versicherten vor unbefugter Kenntnisnahme bis zum 31. Januar 2018 zu erstellen. Die Richtlinie wurde in Abstimmung mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und dem Bundesamt für Sicherheit in der Informationstechnik fristgemäß erstellt und den Krankenkassen mit Rundschreiben vom 6. Februar 2019 bekanntgegeben. Laut der Richtlinie sind die darin gelisteten Anforderungen innerhalb von zwölf Monaten für bestehende Verfahren, also bis zum 6. Februar 2020, umzusetzen.

In der Richtlinie wird u. a. geregelt, welche Anforderungen für eine sichere Authentifizierung des Versicherten durch die Kassen erfüllt werden müssen und wie eine sichere Übermittlung von Daten auf postalischem oder elektronischem Weg zu erfolgen hat.

Gleichzeitig beinhaltet der Referentenentwurf des Patientendaten-Schutzgesetzes des Bundesministeriums für Gesundheit eine Regelung, die der gematik GmbH eine zentrale Rolle bei der sicheren Ausgestaltung der Ausgabeprozesse überträgt und die Anforderungen an die Richtlinie nach § 217f Absatz 4b SGB V verschärft.

   d) Besteht die Möglichkeit, dass der elektronische Personalausweis genutzt werden kann, um eine sichere Authentifizierung von Seiten der Versicherten in der Telematikinfrastruktur zu gewährleisten, und plant die Bundesregierung in diesem Bereich Verfahren zu entwickeln?

Die Nutzung des elektronischen Personalausweises zur Identifizierung und Authentifizierung im Gesundheitswesen, speziell bei Anwendungen in der Telematikinfrastruktur, ist derzeit nicht geplant.

6. Welche Sicherheitsvorkehrungen wurden ergriffen, um zu gewährleisten, dass Konnektoren nicht von unberechtigten Personen bestellt werden können?

Der Besitz eines Konnektors allein berechtigt nicht zum Zugriff auf die Telematikinfrastruktur oder auf eine ihrer Fachanwendungen. Die Forderung nach einem sicheren Auslieferungsprozess rührt aus den Sicherheitsanforderungen des Bundesamtes für Sicherheit in der Informationstechnik, wonach durch eine sichere Lieferkette Manipulationen am Konnektor auf dem Weg bis zum Endnutzer vermieden werden. Die Notwendigkeit einer Einschränkung des empfangsberechtigten Personenkreises wird nicht gesehen.

7. Wie bewertet die Bundesregierung die im eingangs genannten Artikel der „c't“ aufgedeckten Sicherheitslücken in den Konnektoren und Kartenlesegeräten?

Nach Kenntnisstand der Bundesregierung lassen sich aus dem Artikel keine Schwachstellen ableiten, die die Sicherheit des Konnektors gemäß den festgelegten Sicherheitsanforderungen gefährden.

8. Wie bewertet die Bundesregierung die aufgedeckten Verstöße gegen Open-Source-Softwarelizenzen bei dem KoCoBox-Konnektor (vgl. Vorbemerkung der Fragesteller), und welche Maßnahmen wird sie hier ergreifen?

Der Bundesregierung liegen hierzu keine Erkenntnisse vor. Prinzipiell gilt, dass Hersteller von Konnektoren auch die Anforderungen des Urheberrechts beachten müssen.

9. Wie soll sichergestellt werden, dass Konnektoren durch Sicherheitslücken nicht ganze Praxis- oder Kliniknetzwerke gefährden?

Die Konnektoren sind auf einem sehr hohem Niveau durch das Bundesamt für Sicherheit in der Informationstechnik sicherheitszertifiziert. Nach der Zulassung durch die gematik GmbH werden durch den Hersteller und die gematik GmbH zudem regelmäßig Sicherheitsüberprüfungen durchgeführt.

10. Welche Konsequenzen zieht die Bundesregierung aus der in der Zeitschrift „c't“ (3/2020), vgl. Vorbemerkung der Fragesteller, geäußerten Kritik am Common-Criteria-Zertifizierungsprozess, und soll einer statischen Zertifizierung eines Geräts nun eine befristete oder dauerhafte Rezertifizierung von Geräten erfolgen, damit neu auftretende Sicherheitslücken und Erkenntnisse berücksichtigt werden können?

Die Kritik am Common Critieria-Verfahren ist unberechtigt. Alle Updates eines Konnektors werden zwar zugelassen, dies bedeutet jedoch nicht, dass damit auch jedes Mal der gleiche Prüfungsaufwand verbunden ist. Sowohl das Bundesamt für Sicherheit in der Informationstechnik als auch die gematik GmbH können in Abhängigkeit des Änderungsgrades des Updates über die Prüftiefe entscheiden. Für dringende Sicherheitsaktualisierungen sieht § 291b Absatz 1a Satz 11 SGB V zudem vor, dass diese auf Basis einer befristeten Genehmigung ohne vorherige Zulassung ausgebracht werden dürfen. Dies erfolgt in sehr kurzen Zeiträumen bis maximal eine Woche.

Weiterhin beinhaltet der Referentenentwurf des Patientendaten-Schutzgesetzes des Bundesministeriums für Gesundheit eine Regelung, alle Komponenten der Telematikinfrastruktur regelmäßig auf ihre Sicherheit zu überprüfen.

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