Deutscher Bundestag **Drucksache 19/17505**

19. Wahlperiode 03.03.2020

Kleine Anfrage

der Abgeordneten Dr. Wieland Schinnenburg, Michael Theurer, Grigorios Aggelidis, Renata Alt, Christine Aschenberg-Dugnus, Nicole Bauer, Jens Beeck, Dr. Jens Brandenburg (Rhein-Neckar), Mario Brandenburg (Südpfalz), Dr. Marco Buschmann, Britta Katharina Dassler, Dr. Marcus Faber, Daniel Föst, Otto Fricke, Thomas Hacker, Peter Heidt, Katrin Helling-Plahr, Markus Herbrand, Torsten Herbst, Manuel Höferlin, Reinhard Houben, Ulla Ihnen, Olaf in der Beek, Gyde Jensen, Karsten Klein, Dr. Marcel Klinge, Daniela Kluckert, Pascal Kober, Carina Konrad, Konstantin Kuhle, Ulrich Lechte, Alexander Müller, Roman Müller-Böhm, Dr. Martin Neumann, Matthias Seestern-Pauly, Frank Sitta, Judith Skudelny, Dr. Hermann Otto Solms, Bettina Stark-Watzinger, Dr. Marie-Agnes Strack-Zimmermann, Katja Suding, Stephan Thomae, Manfred Todtenhausen, Dr. Florian Toncar, Dr. Andrew Ullmann, Sandra Weeser, Nicole Westig und der Fraktion der FDP

Gewährleistung der Datenhoheit von Versicherten in der Telematikinfrastruktur

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

Wir fragen die Bundesregierung:

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?
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?
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?
   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?
   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?
   d) Plant die Bundesregierung, möglicherweise kompromittierte Ausweise neu auszugeben, wenn ja, wann, und in welchem Umfang?
   e) Welchen Einfluss haben die ergriffenen Maßnahmen auf die Honorarkürzungen gemäß § 291 SGB V?
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?

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?

6. Welche Sicherheitsvorkehrungen wurden ergriffen, um zu gewährleisten, dass Konnektoren nicht von unberechtigten Personen bestellt werden können?
7. Wie bewertet die Bundesregierung die im eingangs genannten Artikel der „c't" aufgedeckten Sicherheitslücken in den Konnektoren und Kartenlesegeräten?
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?
9. Wie soll sichergestellt werden, dass Konnektoren durch Sicherheitslücken nicht ganze Praxis- oder Kliniknetzwerke gefährden?
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?

Berlin, den 12. Februar 2020

Christian Lindner 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