Deutscher Bundestag **Drucksache 19/16949**

19. Wahlperiode 30.01.2020

Kleine Anfrage

der Abgeordneten Maria Klein-Schmeink, Dr. Konstantin von Notz, Dr. Bettina Hoffmann, Dr. Kirsten Kappert-Gonther, Kordula Schulz-Asche, Katja Dörner, Dr. Anna Christmann, Kai Gehring, Erhard Grundl, Ulle Schauws, Charlotte Schneidewind-Hartnagel, Margit Stumpp, Beate Walter-Rosenheimer, Tabea Rößner, Corinna Rüffer und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Schwachstellen bei der Ausgabe von elektronischen Ausweisen und Komponenten der Telematikinfrastruktur im Gesundheitswesen

Mitglieder des Chaos Computer Clubs (CCC) haben am 27. Dezember 2019 beim 36. Chaos Communication Congress in Leipzig Schwachstellen und Sicherheitslücken beim Ausgabeprozess für verschiedene in der Telematikinfrastruktur (TI) genutzte Komponenten und Smartcards demonstriert. Sie konnten zeigen, wie es für Unbefugte problemlos möglich war, einzelne Smartcards und Komponenten der TI durch die jeweiligen beteiligten Serviceprovider zu beziehen (https://e-health-com.de/details-news/ccc-hackt-bestellprozess-gematik-nimmt-stellung/). Es gelang den CCC-Mitgliedern, sich u. a. unautorisiert einen elektronischen Heilberufeausweis und einen Praxisausweis (SMC-B) zu bestellen. Auch ein Konnektor wurde den CCC-Mitgliedern unautorisiert ausgehändigt. Zusätzlich waren bei einem beauftragten Serviceprovider die Kartenanträge von 168 Ärztinnen und Ärzten zeitweise online zugänglich.

Außerdem war es den Mitgliedern des CCC gelungen, unautorisiert eine elektronische Gesundheitskarte der AOK Hessen zu bestellen (https://e-health-com.de/details-news/ccc-hackt-bestellprozess-gematik-nimmt-stellung/). Vor dem Hintergrund, dass bereits 2015 Recherchen des ZDF Schwachstellen bei der Ausgabe der elektronischen Gesundheitskarte offengelegt haben (vgl. Deutsche Apothekerzeitung vom 25. Juni 2015 „Massives Sicherheitsleck bei Gesundheitsdaten“, abrufbar unter https://www.deutsche-apotheker-zeitung.de/news/artikel/2015/06/25/unnamed-75), stellt sich die Frage, warum es noch immer zu derartigen Problemen bei der Ausgabe von elektronischen Ausweisen und Komponenten der Telematikinfrastruktur kommt, die auch im Stande sind, die Akzeptanz der Digitalisierung des Gesundheitswesens zu gefährden.

Wir fragen die Bundesregierung:

1. Wie bewertet die Bundesregierung die durch Mitglieder des CCC offenbarten Schwachstellen und Sicherheitslücken beim Ausgabeprozess für verschiedene in der Telematikinfrastruktur genutzte Komponenten und Smartcards (vgl. https://www.ccc.de/en/updates/2019/neue-schwachstellen-gesundheitsnetzwerk), und teilt die Bundesregierung die Ansicht der Fragesteller, dass diese, sollten sie nicht schnellstmöglich abgestellt werden, im

Stande sind, die Akzeptanz der Digitalisierung des Gesundheitswesens zu gefährden?

2. Welche konkreten Maßnahmen ergreift die Bundesregierung in Kooperation mit den jeweils zuständigen Stellen vor dem Hintergrund der Recherchen von Mitgliedern des Chaos Computer Clubs im Hinblick

   a) auf den Prozess der Ausgabe der elektronischen Gesundheitskarte,

   b) auf den Prozess der Ausgabe von eHBA und SMC-B,

   c) auf den Prozess der Ausgabe von Komponenten wie Konnektoren und Kartenterminals?

3. Wie häufig ist es nach Kenntnis der Bundesregierung Unbefugten bislang gelungen, unautorisiert an bestimmte Karten und Komponenten zu gelangen (bitte detailliert jeweils nach Herausgeber für eGK, eHBA, SMC-B, HSM-B, ggf. gSMC-KT, Kartenterminals und Konnektoren darstellen)?

Wenn die Bundesregierung hierzu noch keine Kenntnisse hat, wann wird sie dem Deutschen Bundestag hierzu einen detaillierten Bericht vorlegen?

4. Wie war zum Zeitpunkt der Recherchen des CCC nach Kenntnis der Bundesregierung der konkrete Ablauf des Kartenherausgabeprozesses für die in der Telematik genutzten Smartcards (bitte detailliert jeweils für eGK, eHBA, SMC-B, HSM-B, ggf. gSMC-KT und getrennt nach den jeweiligen Herausgebern der Karten wie Kassen, Kammern, KVen und KZVen darstellen)?

5. Wie war zum Zeitpunkt der Recherchen des CCC nach Kenntnis der Bundesregierung der konkrete Ablauf des Herausgabeprozesses für die in der Telematik benutzten Komponenten Konnektor und Kartenterminal?

6. Wurden nach Kenntnis der Bundesregierung alle Herausgabeprozesse sowohl für Smartcards als auch für Komponenten im Hinblick auf die zuverlässige und eindeutige Identifizierung der Empfänger von Karten und Komponenten überprüft?

   Wenn ja, wann, durch wen, und mit welchem Ergebnis?

   Wenn nein, warum nicht?

7. Wurde nach Kenntnis der Bundesregierung der Ausgabeprozess für die jeweiligen Karten (eGK, eHBA, SMC-B, HSM-B, ggf. gSMC-KT) spezifiziert (bitte für jede Karte darstellen)?

   Wenn ja, wann, und durch wen?

   Wenn nein, warum nicht, und beabsichtigt die Bundesregierung für die Zukunft eine solche Spezifizierung vorzugeben?

8. Wurde der jeweilige Ausgabeprozess für die jeweiligen Karten zugelassen?

   Wenn ja, wann, und durch wen?

   Wenn nein, warum nicht, und beabsichtigt die Bundesregierung für die Zukunft eine solche Zulassung?

9. a) Welche Verfahren zur sicheren und eindeutigen Identifizierung der Empfängerinnen und Empfänger von Karten und Komponenten gibt es nach Kenntnis der Bundesregierung, und warum wurden diese nicht von vornherein verbindlich als einzig mögliche Verfahren vorgegeben?

   b) Trifft es zu, dass die Bundesnetzagentur unsichere Verfahren wie „BankIdent“ und „KammerIdent“ inzwischen deaktiviert hat (https://e-health-com.de/details-news/ccc-hackt-bestellprozess-gematik-nimmt-st

ellung/), und wenn ja, warum ist dies erst nach den Berichten über die Rechercheergebnisse des CCC geschehen?

10. Wurden die bei der Ausgabe der Karten beteiligten Serviceprovider (Medisign, Bundesdruckerei, T-Systems) nach Kenntnis der Bundesregierung jeweils zugelassen bzw. in anderer Weise überprüft?

    Wenn ja, wann, und durch wen?

    Wenn nein, warum nicht, und beabsichtigt die Bundesregierung für die Zukunft eine solche Zulassung oder zumindest Überprüfung vorzugeben?

11. Ist in Bezug auf Frage 10 nach Kenntnis der Bundesregierung ein Entzug der jeweiligen Zulassung der beteiligten Serviceprovider denkbar, beispielsweise für den Fall, dass diese die bekannt gewordenen Schwachstellen und Sicherheitslücken nicht schnellstmöglich abstellen oder sich im Zuge weiterer Überprüfungen als nicht vertrauenswürdig erweisen?

12. Warum ist es nach Kenntnis der Bundesregierung offenbar noch immer möglich (vgl. https://e-health-com.de/details-news/ccc-hackt-bestellprozess-gematik-nimmt-stellung/), bei einzelnen Krankenkassen durch Adressänderungen ohne eine sichere Identifizierung unbefugt an eine elektronische Gesundheitskarte zu gelangen, obwohl die diesbezüglichen Schwachstellen beim Ausgabeprozess seit langem bekannt sind?

13. a) Welche Maßnahmen haben die Bundesregierung, der GKV-Spitzenverband und die Aufsichtsbehörden der Länder seit 2015 konkret ergriffen, um die Ausgabe von elektronischen Gesundheitskarten an Unbefugte zu verhindern oder zumindest zu erschweren?

    b) Wurde die Umsetzung dieser Maßnahmen durch die Bundesregierung bzw. die Aufsichtsbehörden der Länder überprüft, und wenn ja, wann ,und wie konkret?

    Wenn nein, warum ist dies bislang unterblieben, und ist geplant, dieses schwerwiegende Versäumnis nachzuholen?

14. Kann nach Kenntnis der Bundesregierung mittels eines elektronischen Heilberufeausweises (eHBA) aktuell eine qualifizierte elektronische Signatur (QES) erzeugt werden, und für welche Zwecke kann diese QES derzeit genutzt werden?

15. Welche Angriffsszenarien sind nach Auffassung der Bundesregierung möglich, solange die Gefahr besteht, dass für die Telematikinfrastruktur notwendige Karten und Komponenten weiterhin an Unbefugte ausgegeben werden?

16. Welche konkreten datenschutzrechtlichen Bestimmungen sind nach Auffassung der Bundesregierung in den vom CCC durchgeführten Fällen des unautorisierten Bezuges von Smart Cards und Komponenten der TI einschlägig, um die Verantwortlichkeit der ausgebenden Stellen zu überprüfen und ggf. zu sanktionieren?

17. Wird die Bundesregierung sich im Rahmen ihrer Beteiligungen dafür einsetzen, dass in der Aufarbeitung der vom CCC aufgedeckten Schwachstellen der Ausgabeverfahren die Einbeziehung der Expertise des Bundesbeauftragten für den Datenschutz nachgesucht wird, und wenn nein, warum nicht?

18. Hält die Bundesregierung den gesetzlichen Rahmen als auch die Informationen der verantwortlichen Stellen zur Sicherstellung ausschließlich autorisierter Herausgaben von Smart Cards und TI-Komponenten für ausreichend, und wenn nein, welche Änderungen und Anstöße plant sie zur Verbesserung der gegenwärtigen Situation?

19. Sind Bundesregierung, Gematik, Kartenherausgeber und Komponentenherausgeber oder Serviceprovider nach Kenntnis der Bundesregierung bislang auf die beim 36. Chaos Communication Congress in Leipzig zur Thematik vortragenden oder andere Mitglieder des Chaos Computer Clubs mit der Bitte um Austausch herangetreten?

    Wenn ja, wann, und mit welchem Ergebnis?

    Wenn nein, warum nicht?

20. Plant die Bundesregierung angesichts der bekannt gewordenen Schwachstellen, die Vorgaben für dynamische Sicherheitsstandards zu erhöhen oder zu konkretisieren?

21. Plant die Bundesregierung regelmäßige Pentests, Whitehacking-Programme, finanzierte Bugbounty-Programme oder vergleichbare Maßnahmen, um in Zukunft frühzeitig auf Sicherheitslücken der Telematikinfrastruktur aufmerksam zu werden?

    Wenn ja, welche Überlegungen gibt es bereits hierzu auf Seiten der Bundesregierung oder nach Kenntnis der Bundesregierung auf Seiten der Gematik, Karten- und Komponentenherausgeber und Serviceprovider, wie werden solche Programme konkret ausgestaltet sein, und wann werden diese umgesetzt?

    Wenn nein, warum nicht?

Berlin, den 14. Januar 2020

Katrin Göring-Eckardt, Dr. Anton Hofreiter 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