12993/J
vom 28.04.2017 (XXV.GP)

ANFRAGE

der Abgeordneten Ing. Norbert Hofer, Dr. Dagmar Belakowitsch-Jenewein
und weiterer Abgeordneter
an die Bundesministerin für Gesundheit und Frauen

betreffend ELGA-System

Eine im Auftrag der Wiener Ärztekammer durchgeführte Analyse des Systems und der Funktionalitäten der elektronischen Gesundheitsakte (ELGA) deckt gefährliche Schwachstellen in der Gesamtarchitektur auf. Die Ärztekammer stützt sich bei ihren Erkenntnissen auf eine Studie, die von der renommierten K-Advisors Consulting und Beteiligungsmanagement GmbH durch den IT- und Sicherheitsfachmann Cornelius Dr. Granig und den Cybersecurity-Experten und Geschäftsführer von TS Management Consulting, Dr. Thomas Stubbings, erstellt wurde.

Demnach könne man davon ausgehen, dass ELGA im Besonderen in den nächsten Jahren Ziel von Angriffen sein werde – „oder sogar schon ist", wie Studienautor Dr. Thomas Stubbings von TS Management Consulting betont.

„Neben dem unzweifelhaft wesentlichen Fortschritt, der mit der Einführung eines flächendeckenden elektronischen Systems dieser Art einhergeht, haben sich die Angriffsfläche und die Auswirkungsbreite für potentielle Cyberattacken damit stark erhöht.

Mit einem erfolgreichen Angriff auf einen an ELGA teilnehmenden Gesundheitsdiensteanbieter (GDAs) können nunmehr auf einen Schlag potentiell die Gesundheitsdaten sämtlicher ELGA-Teilnehmer kompromittiert werden, mit möglicherweise dramatischen Folgen – wie Rufschädigung, finanziellen Schäden, bis hin zu Schäden für Leib und Leben. […]

ELGA setzt auf ein dezentrales föderales Identitätsmanagement und Berechtigungskonzept. Dies hat zur Folge, dass die Sicherheit des ELGA Zugangs von der dezentralen Sicherheit jedes einzelnen GDAs abhängt. Ein einziger GDA mit Schwachstellen kann dazu missbraucht werden, potentiell sämtliche ELGA-Gesundheitsdaten aller Österreicher einzusehen, die kein Opt-Out verfügt haben.

[...]

In einer so komplexen Architektur ist das Auftreten von Schwachstellen und in weiterer Folge das fahrlässig oder vorsätzlich herbeigeführte Auftreten von Sicherheitsvorfällen wahrscheinlicher als bei einer zentral gemanagten Architektur mit einheitlichen Sicherheitsstandards und einer konsequenten Security Governance.

Die vorliegenden Dokumente betreffend die Sicherheitskonzepte der zentralen und dezentralen Systeme geben keine hinreichende Vergewisserung über die Belastbarkeit und Resilienz von ELGA aus Sicherheitssicht."

In diesem Zusammenhang stellen die unterfertigenden Abgeordneten, an die Bundesministerin für Gesundheit und Frauen folgende

Anfrage

1. Wieso wurde keine zentrale Benutzerverwaltung für alle ELGA-berechtigte Anwender eingeführt?
2. Weshalb wurde bisher keine verpflichtende separate Authentifizierung beim Einstieg in ELGA durch jeden ELGA-User eingeführt?
3. Warum wurde bisher keine starke Zweifaktor-Authentifizierung, z. B. über die Verwendung von Hardware-Token plus PIN, verwendet?
4. Warum gibt es bisher keine Autorisierung von Batch-Jobs durch eine natürliche Person mittels Zweifaktor-Authentifizierung?
5. Warum werden Kontaktbestätigungen nicht nur nach erfolgter Zweifaktor-Authentifizierung angelegt?
6. Wäre das Stecken der e-Card nicht auch bei Ombudsstellen notwendig?
7. Warum wurde bisher keine flächendeckende digitale Signatur von Gesundheitsdokumenten eingeführt?
8. Ist eine regelmäßige Information an Patienten über sie gespeicherte Daten und deren Abrufe (z. B. über e-Mail oder SMS („Push Service")) künftig vorgesehen?

9. Ist es vorgesehen künftig Informationen an Patienten über erfolgte Kontaktbestätigungen (z. B. über e-Mail oder SMS („Push Service")) weiter zu geben?

10. Werden im gesamten Projekt ELGA Dienstleistungen an externe Unternehmen ausgeschrieben und vergeben?
11. Wenn ja zu Frage 10. Welche Dienstleistungen im Projekt ELGA wurden seit dem Projektstart an welche externen Dienstleister ausgeschrieben und vergeben?
12. Wer wurde per Gesetz für den zukünftigen Betrieb des ELGA Berechtigungssystems (BeS) nominiert?
13. Wer wurde für die technische Umsetzung und den Betrieb des Gesundheitsportals (Zugriff ELGA möglich) beauftragt?
14. Wer ist für den Gesundheitsdienstanbieter-Index (GDA-I) zuständig?
15. Ist durch die Betreiber des Gesundheitsdienstanbieter-Index (GDA-I) eine eindeutige Identifizierung und Authentifizierung der Gesundheitsdienstanbieter möglich?
16. Wer ist für den Patienten-Index (Z-PI) zuständig?
17. Ist durch die Betreiber des Patienten-Index (Z-PI) eine eindeutige Identifizierung und Authentifizierung der Zugriffsberechtigten möglich?
18. Werden sie die Studie „Analyse des Systems Elektronische Gesundheitsakte ELGA" von Dr. Granig und Dr. Stubbings an den Datenschutzrat zur datenschutzrechtlichen Überprüfung vorlegen?
19. In der 218. Sitzung des Datenschutzrates wurde die Umsetzung von ELGA einstimmig gefasst, obwohl es dem Datenschutzrat weder fachlich noch technisch möglich war die damals vorgelegten Implementierungsleitfäden zu ELGA (600 Seiten) ordnungsgemäß zu prüfen. Der Datenschutzrat ging damals von der „Annahme" aus, dass eine entsprechende Überprüfung hinsichtlich der gesetzlichen Rechtsgrundlagen und der datenschutzrechtlichen Vorgaben durch das Bundesministerium für Gesundheit erfolgt ist. Der Datenschutzrat ordnete in weiterer Folge die Prüfung der Implementierungsleitfäden durch das Gesundheitsministerium an. Wurden die Implementierungsleitfäden in Ihrem Ministerium datenschutzrechtlich geprüft und liegt dazu ein datenschutzrechtliches Gutachten ihrer Rechtsabteilung vor?

20. Planen Sie die Durchführung eines Audits der zentralen und Betreiber-Systeme auf Basis der bestehenden Detaildokumente, Interviews mit Key Stakeholdern sowie den Ergebnissen der bisherigen Penetration Tests?
21. Wenn nein, warum nicht?
22. Die A1 Telekom Austria AG bietet Gesundheitsdienstanbietern (GDA) ein A1 ELGA Service (genannt LB A1 ELGA Service) an. Gibt es zu diesen Dienstleistungen der A1 Telekom Austria AG Verträge mit der ELGA-GmbH und dem Gesundheitsministerium?
    Quelle: https://cdn2.a1.net/final/de/media/pdf/LB_A1_ELGA.pdf
23. Sind solche Dienstleistungen externer Dienstleister an Gesundheitsdienstanbieter (GDA) durch die ELGA-GmbH oder das Gesundheitsministerium an die Datenschutzkommission gemeldet worden?
24. Wird der betroffene Patient über den jeweiligen Gesundheitsdienstanbieter (GDA) darüber informiert, wenn seine Befunde und Patientendaten nicht beim GDA selbst, sondern über einen Vertrag bei einem externen Dienstleister, zum Beispiel auf Servern der A1 Telekom AG liegen?
25. Welche weiteren externen Dienstleister für Gesundheitsdienstanbieter (GDA) außer der A1 Telekom AG sind Ihnen bekannt?
26. Haben alle derzeit registrierten Gesundheitsdienstanbieter (GDA) ein gem. §8 GTelG gefordertes IT-Sicherheitskonzept vorgelegt?

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2017-04-28T15:26:19+02:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel
Hinweis	Dieses Dokument wurde elektronisch besiegelt.	