XXIV. GP.-NR
10089 /J
07. Dez. 2011

ANFRAGE

des Abgeordneten Dr. Karlsböck
und weiterer Abgeordneter
an den Bundesminister für Gesundheit

betreffend Informations- und IT-Sicherheitsmanagement der Krankenkassen

Der jüngste Hacker-Angriff der Gruppe Anonymous Austria (AnonAustria) auf die Patientendaten der Tiroler Gebietskrankenkasse (TGKK) spiegelt die Problematik der der Datensicherheit deutlich wieder. Weitere Vorfälle, wie z.B. die „Spitzelaffäre" um die Krankendaten der Landesbeschäftigten in Salzburg, machen das Thema „Datenschutz" hochsensibel. Diese bekannt gewordenen Vorfälle werfen bei den Österreichern als auch bei den Datenschutzexperten berechtigte Zweifel an der Umsicht und Sorgfalt beim Informations- und IT-Sicherheitsmanagement der Krankenkassen auf.

Ein diesbezüglicher online-Artikel, welcher auf der Seite http://futurezone.at/netzpolitik/5167-datenlecks-in-oesterreich-liegt-viel-im-argen.php veröffentlicht wurde, lautet in entsprechenden Auszügen wie folgt:

„(…)„In Österreich liegt leider viel im Argen", kritisiert Datenschützer Hans Zeger von der Arge Daten.
(…)
Immer wieder weisen wir darauf hin, dass viele Systeme nicht einmal die Minimalanforderungen beim Thema Sicherheit beachten. Das ist im Grunde fahrlässig", so Zeger.
(…)
Vom Grundsatz her seien die Datenschutzbestimmungen in Österreich und der EU ausreichend, die großen Defizite ortet Zeger aber in der Umsetzung. „Jedes Auto muss vor der Zulassung geprüft werden. Bei IT-Abteilungen, die für den Schutz von sensiblen Daten zuständig sind, kann eigentlich jeder machen, was er will", kritisiert Zeger. (…)"

In diesem Zusammenhang richten die unterfertigten Abgeordneten an den Bundesminister für Gesundheit folgende

ANFRAGE

1. Verfügen die einzelnen Krankenkassen über ein zeitgemäßes Informations- und IT-Sicherheitskonzept?

2. Wenn nein, warum nicht?

3. Sind diese Informations- und IT Sicherheitskonzepte dokumentiert und auditierbar?

4. Wenn nein, warum sind sie nicht dokumentiert bzw. auditierbar?

5. Entsprechen die Informations- und IT-Sicherheitskonzepte dem Österreichischen Informationssicherheitshandbuch, der Norm ISO/IEC 27001 oder einem anderen anerkannten Informationssicherheitsstandard?

6. Wenn nein, auf welcher Grundlage bauen sie auf?

7. Welche Themenkreise umfassen die Informations- und IT-Sicherheitskonzepte der einzelnen Kassen?

8. Umfassen die Informations- und IT-Sicherheitskonzepte der einzelnen Kassen zumindest alle der nachfolgenden Themenkreise?

   - Sicherheitspolitik und -strategie, Richtlinien
   - Sicherheitsorganisation
   - Klassifizierung
   - Personalsicherheit
   - Physische Sicherheit
   - Sicherheit von Kommunikation und Betrieb
   - Zugriffskontrolle
   - Sicherheit bei Systementwicklung und -wartung
   - Umgang mit Sicherheitsvorfällen
   - Aufrechterhaltung der Betriebsbereitschaft
   - Einhaltung von Sicherheitsvorschriften

9. Wenn nein, warum umfassen sie nicht alle der folgenden Themenkreise?

10. Decken die Informations- und IT-Sicherheitskonzepte der einzelnen Kassen organisatorische, personelle und technische Aspekte gleichermaßen ab?

11. Wenn nein, warum nicht?

12. Wann wurden die Informations- und IT-Sicherheitskonzepte der einzelnen Kassen in den letzten zwei Jahren auf ihre Wirksamkeit geprüft?

13. Wenn nein, warum wurden sie nicht geprüft?

14. Wenn ja, von wem wurden die Informations- und IT-Sicherheitskonzepte der einzelnen Kassen geprüft?

15. Wenn ja, welche Aspekte wurden bei den Informations- und IT-Sicherheitskonzepten der einzelnen Kassen geprüft?

16. Wenn ja, liegen Prüfberichte vor und mit welchen Ergebnissen bzw. Handlungsempfehlungen?

17. Wenn nein, warum nicht?

18. Wurden die ggf. abgegebenen Handlungsempfehlungen aus den Prüfberichten vollständig umgesetzt?

19. Wenn nein, warum nicht?

20. Gibt es bei den einzelnen Krankenkassen Datenklassifizierungsschemen in Bezug auf Vertraulichkeit?

21. Wenn nein, warum nicht?

22. Regeln diese Datenklassifizierungsschemen den Umgang mit Daten von der Übernahme/Anlage bis zu ihrer Löschung/Vernichtung, d.h. über deren gesamten Lebenszyklus hinweg?

23. Wenn nein, warum nicht?

24. Werden §14 und §15 des Datenschutzgesetzes (DSG) 2000 vollständig umgesetzt?

25. Wenn nein, warum nicht?

26. Welche Unterlagen liegen vor, die diese Umsetzung belegen? (z.B. Vertraulichkeitsvereinbarungen, Unterlagen über durchgeführte Sensibilisierungsmaßnahmen, vertragliche Vereinbarungen mit Dritten, Prüfberichte, Konzepte)

27. Wenn nein, warum liegen keine vor?