9896/J
vom 23.02.2022 (XXVII. GP)

Anfrage

der Abgeordneten Mag. Christian Drobits,
Genossinnen und Genossen
an den Bundesminister für Soziales, Gesundheit, Pflege und Konsumentenschutz

betreffend **Datenchaos in Corona-Systemen**

Im Zuge der letzten Monate häuften sich die Datenpannen im BMSGPK. Gerade in einer Pandemie ist der Schutz sensibler Gesundheitsdaten ein wichtiges Thema, wie Gesundheitsminister Mückstein selbst medial immer wieder betont. Trotzdem weckt der Umgang des BMSGPK mit diesen Pannen, den sich dafür interessierenden Journalist*innen, Aktivist*innen und Sicherheitsforschern den Verdacht, dass mehr Arbeit auf das Zudecken als auf das Aufklären dieser Skandale konzentriert wird. Deshalb richten wir folgende parlamentarische Anfrage zur Klärung des Sachverhalts und zur Wiederherstellung des Vertrauens der Bevölkerung an den betroffenen Bundesminister.

Am 16. Dezember 2021 hat derStandard gemeinsam mit der Datenschutz NGO epicenter.works unberechtigte Zugriffe in das Epidemiologische Meldesystem (EMS) aufgedeckt.[1] Im Zuge dieses Skandals wurde auch das Verhältnis der umstrittenen Firma HG Pharma GmbH (HG Labtruck) mit der scheinbaren Nachfolge Firma Novatium GmbH diskutiert. [2] Am 13. Jänner 2022 hat das Magazin ORF Konkret gemeinsam mit der Datenschutz NGO epicenter.works eine Sicherheitslücke in der Plattform oesterreich-testet.at aufgedeckt, über die es allen beteiligten Apotheken möglich war die Gesundheits- und Kontaktdaten von Millionen Menschen einzusehen. Das Vorgehen des BMSGPK gegen den Sicherheitsforscher Gökhan S., der diese Lücke dem BMSGPK in vorbildlicher Manier meldete, führte dazu, dass diese Person ihren Job verlor und genau die falschen Anreize gesetzt werden, um mit Sicherheitslücken künftig verantwortungsvoll umzugehen.[3]

Aus diesen Gründen stellen die unterfertigten Abgeordneten folgende

Anfrage

1. Gibt es eine Protokollierung des Zugriffs in das EMS gemäß § 4 Abs 9 EpiG?
2. Falls ja, wie lange reichen diese Zugriffsprotokolle zurück und beinhalten diese auch die IP-Adressen, von denen aus auf das System zugegriffen wurde?
3. Gab es nach bekannt werden des unberechtigten Zugriffs in das EMS eine Analyse der Protokolldateien, um einen etwaigen Data-Breach gemäß Art. 33 DSGVO oder Manipulation der Daten im EMS festzustellen?

4. Falls ja, von wem wurde diese Analyse durchgeführt und ist diese bereits abgeschlossen?
5. Falls ja, zu welchem Ergebnis kam diese Analyse? Wir ersuchen um Übermittlung des Prüfberichts.
6. Wie viele client-side Zertifikate befinden sich derzeit im Umlauf, die für den Zugriff auf das EMS berechtigt sind?
7. Von wie vielen IP-Adressen aus wurde mittels client-side Zertifikate auf das EMS zugegriffen?
8. Wann und auf wessen Verlangen wurde der Firma Novatium GmbH ein client-side Zertifikat zum Zugriff auf das EMS ausgestellt und wann wurde dieses Zertifikat zum ersten Mal verwendet?
9. Auf welche Person wurde das EMS client-side Zertifikat der Firma Novatium GmbH ausgestellt und handelt es sich dabei um Ralf Herwig oder Joachim Greilberger?
10. Wann wurde das client-side Zertifikat der Firma HG Pharma GmbH zum letzten Mal verwendet?
11. Mit welchem Client Side Zertifikat wurden die PCR-Testergebnisse der HG Pharma GmbH im Rahmen des Programms "Sichere Gastfreundschaft" ins EMS eingetragen?
12. Von wie viel IP-Adressen aus wurde mittels des client-side Zertifikats der Firma HG Pharma GmbH auf das EMS zugegriffen?
13. Die Technikabteilung des BMSGPK hat für das Jahr 2022 eine komplette Neuaufstellung des EMS angekündigt. Wird eine Datenschutz-Folgeabschätzung (DSFA) für dieses neue System durchgeführt?
14. Falls ja, von welchem Dienstleister oder welcher Stelle wird diese DSFA umgesetzt?
15. Falls ja, wird die DSFA veröffentlicht?
16. Ist künftig geplant ein Berechtigungssystem (Access-Control-System) statt den Client-Zertifikaten zu nutzen?
17. Soll ein "EMS neu" auf derselben Infrastruktur wie das Impfregister umgesetzt werden? Wenn nein, warum nicht?
18. Ist das Konzept der "responsible disclosure" im BMSGPK bekannt?
19. Haben die an "Österreich testet" angeschlossenen Apotheken ein IT-Sicherheitskonzept gemäß § 8 GTelG?
20. Wie viele IT-Sicherheitskonzepte nach § 8 GTelG wurden generell seitens des Ministeriums bisher bei Apotheken seit Gültigkeit der Norm im Jahr 2012 überprüft?
21. Wenn bisher nur wenige IT-Sicherheitskonzepte nach § 8 GTelG überprüft wurden: Warum?

22. Was wurde nach bekannt werden einer Sicherheitslücke in oesterreich-testet von Seiten des BMSGPK unternommen?

23. Gab es eine Entschuldigung des BMSGPK oder von BM Mückstein bei Gökhan S.?

24. Ist die Apotheke, für die Gökhan S. arbeitet als er die Sicherheitslücke in oesterreich-testet entdeckt, zum Zeitpunkt des Einlangens dieser parlamentarischen Anfrage noch von oesterreich-testet ausgeschlossen?

25. Welche Anreize setzt das BMSGPK dafür, dass ihm künftige Sicherheitslücken in kritischen Systemen gemeldet werden (Bug Bounty, Schulungen der Kommunikationsabteilung, explizite Kontaktstellen für die Meldung von IT-Sicherheitslücken etc.)?

26. Gab es im Rahmen der Beauftragung von oesterreich-testet an A1/World Direct vertragliche Bedingungen zur IT-Sicherheit und Sicherheitsüberprüfung der Website durch den Auftragnehmer?

27. Gibt es neben Apotheken noch andere Institutionen, die einen Zugriff auf oesterreich-testet hatten, der ihnen das Auslesen von Testdaten ermöglichte, die sie selbst nicht durchgeführt haben?

29. Können Sie ausschließen, dass Daten, die vom dem Impfregister ans EMS übermittelt wurden, von Unbefugten abgerufen wurden?

[1] https://www.derstandard.at/story/2000131971545/massive-sicherheitsluecke-im-zentralen-corona-register-legte-daten-offen

[2] https://www.derstandard.at/story/2000131809617/noch-vor-dem-start-gibt-es-kritik-an-vergabe-der

[3] https://oesterreich.orf.at/stories/3138418/ und https://futurezone.at/netzpolitik/sicherheitsluecke-corona-covid-test-apotheke-gefeuert-webentwickler-oesterreich-testetat/401870441

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2022-02-23T15:58:52+01:00
	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.	