9734/AB
vom 22.04.2022 zu 9896/J (XXVII. GP)

Bundesministerium
Soziales, Gesundheit, Pflege
und Konsumentenschutz

sozialministerium.at

Johannes Rauch
Bundesminister

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrates
Parlament
1017 Wien

Geschäftszahl: 2022-0.152.817

Wien, 22.4.2022

Sehr geehrter Herr Präsident!

Ich beantworte die an meinen Amtsvorgänger gerichtete schriftliche parlamentarische Anfrage **Nr. 9896/J der Abgeordneten Mag. Christian Drobits, Kolleginnen und Kollegen betreffend Datenchaos in Corona-Systemen;** wie folgt:

Fragen 1 und 2:

- Gibt es eine Protokollierung des Zugriffs in das EMS gemäß § 4 Abs 9 EpiG?
- Falls ja, wie lange reichen diese Zugriffsprotokolle zurück und beinhalten diese auch die IP-Adressen, von denen aus auf das System zugegriffen wurde?

Die Protokollierung erfolgt über den Portalverbund (PVP) und das EMS. Somit ist für den zuständigen Portal-Administrator die Rückführung bis zu jener Person möglich, die laut PVP die Anwendung aufgerufen hat. Dies wird im Zuge des Qualitätsmanagements regelmäßig überprüft (siehe § 4 Abs 9 EpiG).

Fragen 3 bis 5:

- 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?
- Falls ja, von wem wurde diese Analyse durchgeführt und ist diese bereits abgeschlossen?
- Falls ja, zu welchem Ergebnis kam diese Analyse? Wir ersuchen um Übermittlung des Prüfberichts.

Nach Bekanntwerden wurde die zuständige Stelle des Bundeslandes informiert, um weitere Maßnahmen zu setzen. Ebenfalls wurden von meinem Ressort als Betreiber Analysen hinsichtlich der Zugriffe durchgeführt. Dadurch konnten die getätigten ZMR-Abfragen festgestellt und detailliert nachvollzogen werden. Dabei konnten alle Abfragen ihrem jeweiligen Zweck eindeutig zugeordnet werden.

Das Vorliegen eines Data Breaches ist aufgrund des Systems, das auf legitimierten Zugriffsberechtigungen basiert, grundsätzlich unwahrscheinlich. Darüber hinaus lag eine unauffällige Anzahl an Labor-Meldungen und ZMR-Abfragen vor. Eine weitere Sicherheitsmaßnahme sind regelmäßige, händisch durchgeführte Datenqualitätschecks bzw. Zugriffsprüfungen.

Aufgrund der sensiblen Gesundheitsdaten und interner Systeminformationen, welche aus Sicherheitsgründen nur eingeschränkten Personen zur Verfügung stehen, ist eine Übermittelung des Prüfberichtes leider nicht möglich.

Fragen 6 und 7:

- Wie viele client-side Zertifikate befinden sich derzeit im Umlauf, die für den Zugriff auf das EMS berechtigt sind?
- Von wie vielen IP-Adressen aus wurde mittels client-side Zertifikate auf das EMS zugegriffen?

Aktuell sind 367 Client-Side-Zertifikate vergeben.
Die Anzahl der verschiedenen IP-Adressen, gezählt seit 01.03.2020 bis heute, von denen aus auf unsere Systeme zugegriffen wurde:

Labor HL7 SS:	1.096
Labor Web GUI:	2.506

Die im Vergleich zur Anzahl der Client-Side-Zertifikate erhöhte Anzahl verwendeter IP-Adressen, lässt sich durch den Umstand erklären, dass viele Labore mit dynamisch zugewiesenen IP-Adresse an das Internet angebunden sind.

Fragen 8 bis 12:

- 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?
- 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?

- Wann wurde das client-side Zertifikat der Firma HG Pharma GmbH zum letzten Mal verwendet?
- Mit welchem Client Side Zertifikat wurden die PCR-Testergebnisse der HG Pharma GmbH im Rahmen des Programms "Sichere Gastfreundschaft" ins EMS eingetragen?
- Von wie viel IP-Adressen aus wurde mittels des client-side Zertifikats der Firma HG Pharma GmbH auf das EMS zugegriffen?

Auf Anfrage des Zuständigen (Labor) wurde am 05.05.2021 ein Zertifikat für die HL7 Schnittstelle von meinem Ressort ausgestellt. Dabei wurde zunächst durch die zuständige Gesundheitsbehörde Kontakt mit dem Zuständigen (Labor) hergestellt. Aus datenschutzrechtlichen Gründen können keine näheren Angaben zu den im Zuge des Antrags übermittelten Daten gemacht werden. Nach Verifikation und Überprüfung der angegebenen Daten wurden die Informationen zum Download an ebendiesen versandt.

Die erste Labormeldung mit diesem Zertifikat ist am 06.05.2021 erfolgt. Auch die letzte Labormeldung wurde am 06.05.2021 getätigt. Seit diesem Zeitpunkt wurden über dieses Zertifikat keine neuen Labormeldungen mehr eingemeldet.
Aufgrund eines neuerlichen Antrages wurde dem Unternehmen in weiterer Folge unter neuem Firmennamen ein neues Zertifikat ausgestellt.

Aus technischen Gründen ist es beim verwendeten Protokoll (HL7 Schnittstelle) nicht möglich, einzelne Meldungen bestimmten Client Side Zertifikaten zuzuordnen.

Fragen 13 bis 17:

- 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?
- Falls ja, von welchem Dienstleister oder welcher Stelle wird diese DSFA umgesetzt?
- Falls ja, wird die DSFA veröffentlicht?
- Ist künftig geplant ein Berechtigungssystem (Access-Control-System) statt den Client-Zertifikaten zu nutzen?
- Soll ein "EMS neu" auf derselben Infrastruktur wie das Impfregister umgesetzt werden? Wenn nein, warum nicht?

Im Zuge des Projekts „EMS neu“ wird eine Evaluierung zur Ermittlung der bestmöglichen technischen Lösung sowohl in Bezug auf das Berechtigungssystem als auch auf die zu nutzende Infrastruktur durchgeführt. Dabei werden hinsichtlich des Berechtigungssystems auch verschiedene Varianten eines Access-Control-Systems in Betracht gezogen sowie hinsichtlich der zu nutzenden Infrastruktur jene des Impfregisters geprüft. Ergänzend dazu wird eine DSFA für das „EMS neu“ von einer noch zu benennenden Stelle durchgeführt und der Öffentlichkeit zur Verfügung gestellt werden.

Frage 18 und 23:

- Ist das Konzept der "responsible disclosure" im BMSGPK bekannt?
- Gab es eine Entschuldigung des BMSGPK oder von BM Mückstein bei Gökhan S.?

Das Konzept des „responsible disclosure“ ist ein gängiges Vorgehen, um sowohl die Sicherheit aller Parteien zu gewährleisten als auch die Sicherheit der Systeme verbessern zu können.

Alle getroffenen und zu treffenden Maßnahmen unterliegen nach bestehender Datenschutzvereinbarung der jeweiligen Apotheke. Der Apotheke als Auftraggeberin des IT-Dienstleisters obliegt es auch Maßnahmen zu setzen. Meinem Ressort kommt diesbezüglich keine Zuständigkeit zu.

Fragen 19 bis 21:

- Haben die an "Österreich testet" angeschlossenen Apotheken ein IT-Sicherheitskonzept gemäß § 8 GTelG?
- Wie viele IT-Sicherheitskonzepte nach § 8 GTelG wurden generell seitens des Ministeriums bisher bei Apotheken seit Gültigkeit der Norm im Jahr 2012 überprüft?
- Wenn bisher nur wenige IT-Sicherheitskonzepte nach § 8 GTelG überprüft wurden: Warum?

Mein Ressort ist lediglich Auftragsverarbeiter. Da dies eine gesetzliche Vorgabe ist und die jeweilige Apotheke datenschutzrechtlicher Verantwortlicher liegt dies im Verantwortungsbereich der jeweiligen Apotheke.

Frage 22:

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

Die Meldung von Sicherheitslücken wird seitens meines Ressorts immer sehr ernst genommen und einer genauen Prüfung sowie Risikobewertung unterzogen. Aufbauend auf dieser Risikobewertung wurde im konkreten Fall sofort ein Konzept zur Behebung der Sicherheitslücke entwickelt und umgehend die Entwicklung der dafür notwendigen technischen Komponenten veranlasst. Nach Abschluss dieser Tätigkeiten wurde das System einer erneuten Sicherheitsüberprüfung unterzogen, bei der keine Mängel festgestellt wurden.

Frage 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?

Die Apotheke selbst war im Sinne einer flächendeckenden Versorgung zu keinem Zeitpunkt von der Softwarelösung und dem Angebot ausgeschlossen. Mein Ressort forderte allerdings eine Stellungnahme zu dem Vorfall über die österreichische Apothekerkammer ein.

Fragen 25 und 26:

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

Mitarbeiter:innen werden laufend anhand ihres Aufgabengebietes geschult; ebenfalls werden Sicherheitsüberprüfungen von Systemen durchgeführt. Darüber hinaus werden meine Mitarbeiter:innen hinsichtlich Meldungen von Sicherheitslücken eingehend sensibilisiert und gehen nach dem unter Frage 22 geschilderten Verfahren verantwortungsvoll mit den erhaltenen Informationen um.

Die Projektunterlagen von oestereich-testet sehen vor, dass die IT-Sicherheit insbesondere mit Blick auf die verarbeiteten, sensiblen Gesundheitsdaten, zu gewährleisten ist und die dafür notwendigen Sicherheitsüberprüfungen entsprechend vorzunehmen sind.

Frage 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?

Grundsätzlich handelt es sich bei oesterreich-testet um ein reines Erfassungssystem, das kein generelles Auslesen von Testdaten ermöglicht. Lediglich der Einbringer kann die von ihm selbst eingemeldeten Tests für einen begrenzten Zeitraum von vier Wochen einsehen, nicht aber die von anderen eingemeldeten Testergebnisse.

Frage 29 (eigentlich Frage 28):

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

Da es sich beim EMS um ein Behördensystem handelt, haben nur dazu berechtigte Personen Zugriff. Sie unterliegen dabei den allgemeinen Vorgaben hinsichtlich der Nutzung des Portalverbundes. Darüber hinaus dürfen sie nur im Rahmen ihrer gesetzlich übertragenen Aufgaben auf das EMS zugreifen (siehe § 4 Abs 9 EpiG). Da es sich beim EMS

um eine Anwendung der Sicherheitsklasse 3 handelt, müssen die entsprechenden Vorgaben eingehalten werden, die unter anderem eine sichere Arbeitsumgebung und eine Zwei-Faktor-Authentifizierung vorschreiben. Letztlich muss jeder Zugriff auch protokolliert werden und unterliegt somit einer laufenden Überprüfung.

Mit freundlichen Grüßen

Johannes Rauch

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR SOZIALES, GESUNDHEIT, PFLEGE UND KONSUMENTENSCHUTZ @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz
	Datum/Zeit	2022-04-22T16:08:53+02:00
	Aussteller-Zertifikat	CN=a-sign-corporate-05,OU=a-sign-corporate-05,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	2098721075
Hinweis	Dieses Dokument wurde amtssigniert.	
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: https://www.sozialministerium.at/site/Ministerium/Willkommen_im_Ministerium/Amtssignatur/Amtssignatur	

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2022-04-22T16:13:11+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.	