6588/J
vom 10.05.2021 (XXVII. GP)

ANFRAGE

der Abgeordneten Dr. Dagmar Belakowitsch, Peter Wurm, Mag. Gerhard Kaniak, Mag. Christian Ragger
und weiterer Abgeordneten
an den Bundesminister für Soziales, Gesundheit, Pflege und Konsumentenschutz
betreffend **E-Card wird zur Sicherheitslücke beim Grünen Pass**

Die Tageszeitung „Kurier" berichtet am 7. Mai 2021:

eCard wird zur Sicherheitslücke beim Grünen Pass

Durch die Kartennummer auf der eCard kann man mit geringem technischen Aufwand den Corona-Status aller Personen in Österreich abfragen.

Der Grüne Pass soll in Österreich schon bald verwendet werden, um bei Veranstaltungen, im Restaurant oder beim Friseur seinen Corona-Status nachzuweisen. Geimpfte, Genesene und Getestete bekommen bei „grün" Zutritt. Doch das in Österreich geplante System ist, wie interne Dokumente zur geplanten Umsetzung zeigen, sehr problematisch. „Es gibt gravierende Privatsphäreprobleme und Sicherheitslücken", heißt es seitens der Bürgerrechtsorganisation epicenter.works, die die Dokumente gemeinsam mit der ZIB2 vorab zugespielt bekam.

eCard-Nummer auf der Rückseite

Dabei haben die Datenschützer mehrere Probleme identifiziert: Eines davon betrifft die eCard. Die Kartennummer, die auf der Rückseite zu finden ist, soll der Schlüssel für die Abfrage des Covid-Statuses der Österreicher*innen werden. Die Nummer besteht aus 20 Zeichen, wobei die ersten 10 Zeichen fix vergeben sind. Beim Eintritt ins Restaurant wird in einer WebApp namens „Greencheck" diese Nummer eingescannt. In Folge bekommt man angezeigt, ob eine Person „grün" oder „rot" ist und ins Lokal darf, oder nicht.

"Wer ein Foto der eCard macht, kann den Status jederzeit erneut abfragen", sagt Thomas Lohninger, Geschäftsführer von epicenter.works in der ZIB2. Weil es sich bei „Greencheck" um eine WebApp handelt, ist das System außerdem anfällig für Massenabfragen. Es ist damit ein massenhaftes, automatisiertes Abrufen von Daten aller sozialversicherten Personen in Österreich möglich. Mit geringem technischen Aufwand kann damit der Corona-Status einer Person aus einem zentralen System abgefragt werden", schreibt epicenter.works in einem Blogposting.

Selbst wenn die Nummern auf der eCard zufällig angeordnet sein würden, würde man damit die Covid-Nachweise aller Sozialversicherten innerhalb eines Monats kopiert haben, heißt es. Bei größerer „krimineller Energie" und mit einem Botnet könnten diese Daten bereits „nach wenigen Tagen" abgegriffen werden, warnt epicenter.works. Bei Corona-bezogenen Daten handelt es sich noch dazu um sensible Gesundheitsdaten, die eigentlich besonders schützenswert sind.

„Im Mai oder Anfang Juni mit diesem System live zu gehen, wäre aus unserer Sicht schwer fahrlässig."

"Schwer fahrlässig"

Die Datenschützer raten daher vom Einsatz dieses Systems vehement ab. „Alles, was in Österreich über die letzten Monate entwickelt wurde, ist eigentlich bei weitem nicht in dem Zustand, um es mit den Echtdaten der Bevölkerung zu befüllen. Im Mai oder Anfang Juni mit diesem System live zu gehen, wäre aus unserer Sicht schwer fahrlässig", heißt es. Die Sicherheitsschwachstelle habe man nur „mit einem kurzen Blick auf die Architektur" sofort als solche identifizieren können.

Ein massenhaftes Abfragen könnte man zwar rein technisch betrachtet mit dem Einsatz von sogenannten Captchas verhindern, aber das wäre im Einsatz bei Veranstaltungen, Friseur oder in Restaurants nicht praktikabel. Schließlich können Personen in so einem Setting nicht einfach noch rasch ein Captcha eingeben, bevor man den einzelnen der Einlass gewährt wird und in der Schlange dahinter weitere Personen warten.

Keine Stellungnahme

Eine Stellungnahme seitens des Gesundheitsministeriums, oder seitens der Sozialersicherungsanstalt gibt es laut "ZIB2" derzeit aktuell nicht. Man sagte lediglich, dass sich das Projekt derzeit im Projektstatus befinde und man "höchste Sicherheits- und Datenschutzstandards" einhalte.

Zentrale Stelle sammelt, wer wo war

Doch es gibt auch aus Datenschutz-Sicht noch mehr an der geplanten Lösung zu kritisieren: Die Abfrage des Corona-Statuses geschieht nämlich bei einem zentralen Online-System, und nicht etwa offline direkt am Gerät. Der "GreenPass" ist eine Web-App. Das bedeutet, dass jede Abfrage des Corona-Statuses in Österreich zentrale erfasst wird.

„Diese Abfrage lässt sich einer geprüften Person und einem Prüfzeitpunkt zuordnen und geht von dem Smartphone der Betriebsstätte aus. Damit kann an dieser zentralen, von der Verwaltung betriebenen Stelle für alle Bereiche des sozialen Lebens, in denen ein Covid-Nachweis als Eintrittstest vorausgesetzt werden, zugeordnet werden, wer wann wo war."

Epicenter.works kritisiert, dass so viel Information an einer Stelle niemals verhältnismäßig sein könne. "Insbesondere, weil es datenschutzfreundlichere Alternativen gäbe und diese auf EU-Ebene vorangetrieben und teilweise als fertige Software zur Verfügung gestellt werden", so die Organisation.

"Explizit nicht zur Umsetzung empfohlen"

Das EU-Parlament hat ebenso wie der österreichische Datenschutzrat als entscheidendes Kriterium für eine Zustimmung zum Grünen Pass der „Unbeobachtbarkeit des Verhaltens der Nutzer*innen" festgelegt, also eine dezentrale Verifikation des Corona-Statuses. Alles andere würde einer unverhältnismäßigen

Überwachung der Bürger*innen gleichkommen. „Aufgrund des eleganten, dezentralen, internationalen Ansatzes sollte die Notwendigkeit für eine zentrale, nationale Datenbank mit allen Nachweisen auf Vorrat hinterfragt werden und wird explizit nicht zur Umsetzung empfohlen", so epicenter.works.

eCard wird zur Sicherheitslücke beim Grünen Pass (msn.com)

In diesem Zusammenhang richten die unterfertigten Abgeordneten an den Bundesminister für Soziales, Gesundheit, Pflege und Konsumentenschutz folgende

ANFRAGE

1) Wie beurteilen Sie die Frage des Datenschutzes und der Datensicherheit im Zusammenhang mit der Verwendung der E-Card beim „Grünen Pass"?
2) Wie beurteilen Sie die Stellungnahme von Herrn Thomas Lohninger, Geschäftsführer von epicenter.works zu Fragen des Datenschutzes und der Datensicherheit im Zusammenhang mit der Verwendung der E-Card beim „Grünen Pass"?
3) Warum hat das Gesundheitsministerium auf Anfrage des ORF am 6. Mai 2021 keine Stellungnahe im Zusammenhang mit dem Datenschutz und der Datensicherheit im Zusammenhang mit der Verwendung der E-Card beim „Grünen Pass" abgegeben?
4) In welchem Stadium befindet sich derzeit das Projekt „Grüner Pass"?
5) Bei wem ist dieses Projekt „Grüner Pass" organisatorisch, personell und finanziell angesiedelt?
6) Welche Rolle und Funktion hat dabei das Bundesrechenzentrum?
7) Welche Rolle und Funktion dabei die ELGA-GmbH?
8) Welche Rolle und Funktion hat dabei der Dachverband der Sozialversicherungsträger?
9) Welche Rolle und Funktion hat dabei das Gesundheitsministerium?
10) Welche Sektion, Gruppe bzw. Abteilung kümmert sich im BMSGPK um den „Grünen Pass"?
11) Wer kümmert sich in Ihrem Kabinett um den „Grünen Pass"?

10.5.

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2021-05-10T16:11:23+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.	