
Ctrl-Alt-R

Wie sicher ist der digitale Impfausweis?

Das Portal Meineimpfungen.ch könnte bald grosse Bedeutung im Alltag erhalten – und Covid-Immunisten mehr Freiheiten ermöglichen. Leider ist die Plattform des Bundes veraltet und enthält einige gefährliche Schwachstellen.

Von [Adrienne Fichter](#) und [Patrick Seemann](#), 19.01.2021

Die Pandemie deckt schonungslos alle Defizite des Gesundheitswesens im digitalen Bereich auf. Angefangen mit dem [Faxgate des Bundesamts für Gesundheit \(BAG\)](#) über [verspätete IT-Beschaffungen](#) bis zu Pannen bei der [Impfanmeldung in den Kantonen](#).

Und auch der [digitale Impfausweis](#) erfüllt keine zeitgemässen Standards an Sicherheit und Datenschutz, wie eine Recherche der Republik zeigt.

Die Plattform Meineimpfungen.ch fristete bisher ein kümmerliches Dasein. [2016](#) waren gerade mal etwas mehr als [100'000 Nutzerinnen](#) [verzeichnet](#). Gross beworben wurde der freiwillige Impfausweis nicht, lediglich über Broschüren in Arztpraxen. Doch seit letztem Sommer [verzeichnet die Website](#), seit kurzem bekannt als «der digitale Impfausweis», einen steilen Anstieg bei den Nutzerzahlen. Im Spätherbst hatten sich bereits [300'000 Personen](#) für einen digitalen Impfausweis angemeldet. Die Anwendungsszenarien sind zwar noch unklar, doch denkbar wäre etwa, die [dazugehörige App als Reise-Freipass](#) zu nutzen: Wer sie hat, darf über die Grenze.

Das BAG lancierte die Website 2011, was sich auch im Design widerspiegelt. Wer ein Konto errichtet, findet eine [komplizierte Benutzerführung](#) vor, die vor allem auf Fachpersonen wie Ärztinnen oder Altersheimpersonal ausgerichtet ist. Ein Bürger, der nur mal schnell seinen Impfausweis digitalisieren will, wird mit den zahlreichen medizinischen Fachbegriffen schnell überfordert sein.

Dieser Umstand allein wäre nicht allzu tragisch. Doch es gibt noch weit schwerwiegendere Missstände.

Etwa beim Thema Datenschutz.

Nutzerinnen werden nur spärlich informiert

Impfdaten gehören zu den besonders schützenswerten Daten. Es erstaunt daher, dass die Datenschutzerklärung von Meineimpfungen.ch sehr kurz und knapp ausfällt. Noch erstaunlicher ist die Antwort des Stiftungsratsmitglieds Hannes Boesch auf die Frage, weshalb dies so ist: «Wir betreiben keine Datenwirtschaft und sind nicht gewinnorientiert. Wir können unsere Datenschutzerklärung deshalb kurz und knapp halten.»

Der Fakt, dass kein gewinnorientiertes Datenunternehmen die Plattform betreibt, soll also ausreichen als Garantie, dass mit diesen Daten nichts Böses angestellt wird, ja, dass deren Verwendung gar nicht weiter erklärt werden muss. Das ist eine durchaus eigenwillige Haltung.

In der Datenschutzerklärung wird zum Beispiel nicht auf die von der Republik identifizierten Tracker hingewiesen, die Statistikdaten über die Zugriffe auf die Website sammeln. Diese Tracker arbeiten zwar gemäss Datenschutzerklärung mit anonymisierten Daten. Aber: Zumindest zum Zeitpunkt, als dieser Beitrag geschrieben wurde, übermittelte die Website auch ganze Benutzernamen an die Tracker der IT-Firma. Eine vollständige «Anonymisierung» sieht anders aus.

Es stimmt zwar: Seit 2015 verantwortet kein Unternehmen, sondern eine Stiftung die Plattform. Einsitz haben darin Vertreter des Ärzteverbands FMH, des Verbands Pharmasuisse und auch des IT-Unternehmens Arpage. So ist Hannes Boesch, der als Stiftungsratsmitglied Medienanfragen beantwortet, gleichzeitig auch CEO von Arpage.

Das Unternehmen Arpage hat Meineimpfungen.ch nicht nur entwickelt, sondern betreibt auch die Datenbank. «Hoch sicher», wie Boesch versichert. Die Impfdatenbank liegt also in den Händen einer privaten Firma. «Die Arpage AG gewährleistet die Datensicherheit insbesondere durch die fortlaufende Überwachung und Verbesserung von Prozessen und dem System zur Datenbearbeitung», so Boesch.

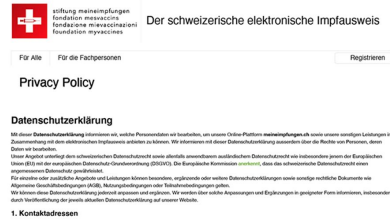
Doch gerade in Sachen Datensicherheit gab es bis vor kurzem grossen Verbesserungsbedarf:

- Die Republik fand etwa heraus, dass sich im Supportbereich der Plattform **eine bekannte Schwachstelle**, die SQL Injection, befindet. Es handelt sich um eine Schwachstelle, die schon seit drei Jahren bekannt ist. Eine Angreiferin könnte sich durch diese Sicherheitslücke direkten Zugriff auf Datenbanken verschaffen und eigene Befehle ausführen. Sprich: im schlimmsten Fall Impfdaten von fremden Personen manipulieren. Es ist unklar, für wen dieser Supportbereich genau gedacht ist und ob man damit im schlimmsten Fall persönliche Daten extrahieren kann. Denn ausprobieren darf das die Republik nicht, wenn sie nicht gegen geltende Gesetze verstossen will. Die Frage bleibt: Können Hacker damit von aussen auf die Impfdatenbank zugreifen? Boesch sagt: «Wir können ausschliessen, dass über die Supportseiten auf Impfdaten zugegriffen werden kann.» Doch Arpage musste auf unseren Hinweis zuerst weitere Abklärungen treffen, was das Ausmass der Schwachstelle angeht.
- Der Zugriff auf Meineimpfungen.ch war mit **veralteten unsicheren Sicherheitsprotokollen** wie TLS 1.0 und TLS 1.1 möglich, wie Recherchen der Republik zeigen. TLS ist ein Verschlüsselungsprotokoll zur Datenübertragung im Internet. Das zeitgemässe TLS 1.3 hingegen wurde nicht unterstützt. Ausserdem war die Plattform unzureichend gegen sogenannte Cross-Site-Scripting-Attacks geschützt, was es einer Angreiferin grundsätzlich erlaubt hätte, über eine Drittseite die im Browser angezeigten Impf- und Kontaktdaten mitzulesen. Die Republik konfrontierte die Stiftung auch mit diesem Befund. Boesch verteidigte erst den Einsatz von veralteten TLS-Protokollen mit der Begründung, den Zugriff auch älteren Browsern ermöglichen zu wollen. Doch seither hat die Stiftung einige Hausaufgaben gemacht: Das alte TLS-Protokoll 1.0/1.1 wurde deaktiviert. Inzwischen erfolge der Zugriff nur noch mit TLS 1.2, so Boesch. Der Zugriff via TLS 1.3 soll ebenfalls bald möglich sein, und man werde ein besonderes Augenmerk auf Angriffe aller Art richten, einschliesslich Cross-Site-Scripting-Attacks. Sicherheits-

überprüfungen würden wöchentlich von der Firma Netchange Informatik vorgenommen, sagt Boesch.

Ob diese Audits ausreichen, wird nicht zu erfahren sein. Die Software der Plattform ist nicht quelloffen, sie lässt sich also nicht einsehen und auf Schwachstellen prüfen. Da es weder eine Offenlegungspflicht noch eine Meldepflicht für allfällige Angriffe gibt, muss man sich in Sachen IT-Security auf die Aussagen der Stiftung verlassen.

Was immerhin von aussen sichtbar ist: Seit der Anfrage der Republik wurde die Datenschutzerklärung um einige Punkte angepasst.



Die Datenschutzerklärung vor der Anfrage der Republik (links) und nach der Anfrage.

Auch ein paar weitere einfache Details wurden zwischenzeitlich angegangen.

Noch vor zwei Wochen erzielte Meineimpfungen.ch bei einschlägigen Bewertungstools keine Bestnoten, im Gegenteil: Das Observatory-Tool der Stiftung Mozilla verpasste dem digitalen Impfausweis in Sachen IT-Sicherheit ein «F»: ungenügend. Zwischenzeitlich wurden einige Verbesserungen getätigt, wie etwa die Aktivierung von HSTS: Damit wird die Verschlüsselung des Datenverkehrs zwischen dem Browser der Nutzerin und der Website Meineimpfungen.ch sichergestellt.

Die Impfungen sind in allen Kantonen angelaufen, die Nachfrage ist gross. Doch in Sachen digitale Prävention gegen böswillige Hacker gibt es noch einiges zu tun.

