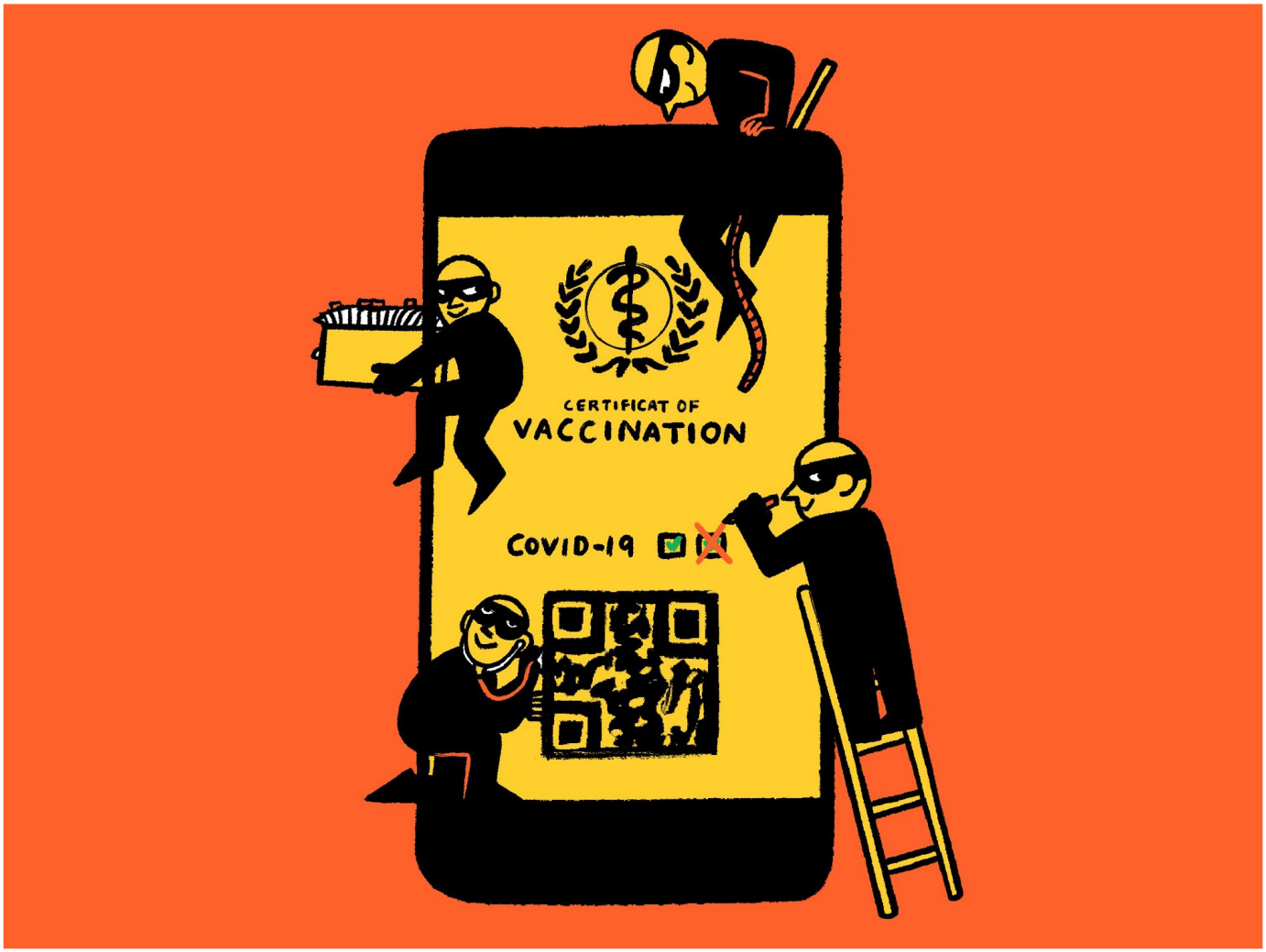

Wollen Sie wissen, womit Viola Amherd geimpft ist?

Offen wie ein Telefonbuch und leicht manipulierbar: Um die Sicherheit und den Datenschutz beim digitalen Schweizer Impfausweis steht es schlimmer als bisher bekannt. Selbst die Impfdaten von Bundesräten waren für die Republik zugänglich.

Eine Recherche von Adrienne Fichter, Patrick Seemann (Text) und Lisa Rock (Illustration), 23.03.2021, Updates 30.03.2021, 31.05.2022

Wer gegen Covid-19 geimpft ist, soll in Europa frei reisen können. Diese Idee wird derzeit in der EU diskutiert. Nach dem Vorbild von Israel möchte die Europäische Union einen «digitalen grünen Impfausweis» einrichten.

Auch die Schweiz arbeitet an einem digitalen Impfausweis. Das Parlament hat dafür vergangene Woche das Covid-19-Gesetz angepasst.

Dabei sind alle Augen auf die Plattform Meineimpfungen.ch und die dazugehörige Impf-App MyViavac gerichtet. Nutzerinnen können dort eintragen, welche Impfungen sie wann erhalten haben, und überprüfen, ob ihnen gewisse Impfungen fehlen.

Die Plattform wird von einer Stiftung betrieben und vom Bundesamt für Gesundheit (BAG) für den elektronischen Impfausweis favorisiert. Neun Kantone haben einen Vertrag mit der Stiftung. Der Zweck: die Zusammenführung der Daten der Impfanmeldungssoftware der Kantone und des gesamtschweizerischen elektronischen Impfbüchleins.

Doch Meineimpfungen.ch und das zugehörige MyCovidVac-Modul weisen gravierende Sicherheitsmängel auf und erfüllen die Anforderungen an den Datenschutz nicht. Ein technischer Bericht der Informationssicherheitsexperten Sven Fassbender, Martin Tschirsich und André Zilch sowie Recherchen der Republik bringen drei gravierende Probleme zum Vorschein:

1. **Umfassende Zugriffsrechte:** Jede Medizinfachperson, die auf der Plattform registriert ist, hat umfassenden Zugriff auf die Impf- und Gesundheitsdaten sämtlicher erfasster Privatpersonen. Sie könnte zum Beispiel deren covidrelevante Impfdaten einfach manipulieren.
2. **Mangelhafte Überprüfung:** Bei der erstmaligen Anmeldung als Medizinfachperson findet keine eigentliche Identitätsprüfung statt. Die Verifikation basiert allein auf den Informationen des Antragstellers. Das bedeutet: Es ist einfach, sich als «Arzt» auszugeben.
3. **Sicherheitslücken:** Hackerinnen können relativ leicht die Covid-19-Impfausweise sämtlicher bisher geimpfter Personen auf der Plattform erbeuten. Mit etwas technischem Wissen können sie ausserdem die Impfdaten und weitere Gesundheitsdaten manipulieren.

Das Tor für Missbrauch und Kompromittierung der Daten von rund 450’000 eingetragenen geimpften Personen, darunter von 240’000 Covid-Geimpften, ist mit den festgestellten Sicherheitslücken sperrangelweit offen.

Bereits im Januar 2021 berichtete die Republik über Sicherheitsmängel bei Meineimpfungen.ch. Damals ging es um technische Fragen, die teilweise behoben wurden. Eine vertiefte Überprüfung der Plattform zeigte nun aber, dass die Probleme viel gravierender sind als angenommen. Und sie stellt die Tauglichkeit der Plattform als solche infrage.

«Wir stufen das Risiko eines Missbrauchs als kritisch ein», sagt Sicherheitsexperte Sven Fassbender. Mit «kritisch» ist in der Fachwelt das höchste Sicherheitsrisiko gemeint. Und das bedeutet: Die Schwachstellen sind auch von Laien ausnutzbar. Das Expertenteam schreibt in seinem Bericht dazu: «Die Dienste müssen unverzüglich ausser Betrieb genommen werden.»

Ob die Sicherheitslücken tatsächlich von Kriminellen ausgenutzt worden sind, ist unklar. Doch das Risiko ist real: Die Bundesräte Ignazio Cassis und Viola Amherd haben auf Meineimpfungen.ch einen Account, wie die Republik herausgefunden hat. Und die Republik hätte ohne weiteres den Impfstatus der Bundesräte sowie Angaben über chronische Krankheiten einsehen können, ohne dass Aussenminister Cassis und Verteidigungsministerin Amherd etwas davon mitbekommen hätten.

Der eidgenössische Datenschutzbeauftragte (Edöb) Adrian Lobsiger hat aufgrund des Sicherheitsberichts und der Republik-Recherchen umgehend ein Aufsichtsverfahren gegen die Stiftung Meineimpfungen.ch eingeleitet.

Die Plattform wurde gestern Montag vom Netz genommen.

1. Die Impfdaten sind offen wie ein Telefonbuch

Von aussen betrachtet wirkt bei Meineimpfungen.ch alles normal. Die Daten des elektronischen Impfpasses scheinen nur für Nutzer selbst zugänglich zu sein. Damit eine medizinische Fachperson diese Daten einsehen kann, muss sie dieser explizit den Zugriff freischalten oder einen Code übermitteln.

Anders präsentiert sich das aus Sicht der registrierten Fachperson: Sie hat ohne weitere Hürden Zugriff auf die persönlichen Daten sämtlicher auf der Plattform registrierter Privatpersonen. Dies hat die Republik bei den Covid-19-Impfungen herausgefunden. Andere Impfdaten – wie die gegen Windpocken oder Masern – wurden aus rechtlichen Gründen nicht angeschaut.

Das bedeutet also:

- Persönliche Informationen wie Adresse, Telefonnummer, Geburtsdatum, Impfstatus, Krankenkassendetails sowie besonders schützenswerte Personendaten wie Impfstatus oder Risikofaktoren von registrierten Bürgerinnen können von allen medizinischen Fachpersonen eingesehen und geändert werden. Für sie ist die Plattform ein offenes Telefonbuch, das sie erst noch umschreiben können.
- Auch die sogenannten Indikatoren für eine Covid-19-Impfung sind für die Mediziner sichtbar und auch veränderbar: Damit ist es etwa ohne Wissen der Betroffenen möglich, eine kerngesunde 25-Jährige in die Risikogruppe zu verschieben (und ihr so eine frühe Impfung zu sichern) oder im umgekehrten Fall bei einem 72-Jährigen die Vorerkrankungen zu streichen, um den Impftermin hinauszuzögern.

Das ist ein gravierender konzeptioneller Sicherheitsmangel. Ob es auch möglich wäre, eine Covid-19-Impfung einzutragen, die es nie gab, hat die Republik aus rechtlichen Gründen nicht ausprobiert. Doch nur schon die Tatsache, dass jede als Fachperson registrierte Benutzerin besonders schützenswerte Gesundheitsdaten aller erfassten Nutzer schweizweit einsehen und abändern kann, ist kritisch genug. «Das verstösst auf krasse Weise auch gegen die Nutzungsbedingungen von Meineimpfungen.ch», sagt der eidgenössische Datenschutzbeauftragte Adrian Lobsiger zur Republik.

Schlimmer noch: Covid-19-kritische Ärzte könnten sich an den Informationen zu schaffen machen und die Impfdatensätze von Patientinnen manipulieren.

2. Jeder kann sich als Fachperson registrieren lassen

Noch gravierender als die Lese- und Modifikationsrechte für Ärztinnen ist, dass die Registrierung als medizinische Fachperson anfällig für Betrug ist. Hackerinnen können sich mit wenigen Kniffen auf Meineimpfungen.ch als Fachperson registrieren und dieselben Zugriffsrechte wie Ärzte erhalten.

Auch hier sieht der Registrierungsprozess zunächst sicher aus:

-

Als medizinische Fachperson meldet man sich mit seiner EAN/GLN-Identifikation (eine eindeutige Identifikationsnummer von Ärztinnen) und persönlichen Daten und Telefonnummer/E-Mail für einen Account an.

– Anschliessend erhält man von der Plattform eine E-Mail mit der Bitte, sich als medizinische Fachperson auszuweisen, sei das mithilfe eines Fotos des – vom Ärzteverband FMH vergebenen – HPC-Ausweises oder der Urkunde oder des Diploms. Erst dann wird das Benutzerkonto freigeschaltet.

Das klingt nach einer seriösen, sicheren Prüfung.

Doch das schweizerische EAN/GLN-Verzeichnis ist öffentlich verfügbar, man kann sich also problemlos den Namen einer Fachperson heraussuchen, von der man annehmen kann, dass sie bisher noch keinen Zugang zur Impfplattform beantragt hat, und sich als diese Person anmelden.

Die Republik hätte also ohne grossen Aufwand einen fingierten Zugang zu Meineimpfungen.ch erstellen können: anhand eines Ärztenamens und der passenden EAN/GLN-Nummer und einer eigens zu diesem Zweck kreierten E-Mail-Adresse. Der erforderliche Nachweis der medizinischen Ausbildung hätte relativ leicht mit einem gefälschten Dokument beziehungsweise Fotos erbracht werden können. Beispiele für Health-Professional-Card-Ausweise wie auch für medizinische Berufsdiplome finden sich leicht im Internet.

Die Zugangsprüfung für medizinische Fachpersonen basiert also auf reinem Vertrauen – darauf, dass der sich anmeldende Arzt tatsächlich die Person ist, als die er sich ausgibt. Bessere Verfahren zur Überprüfung sind nicht vorgesehen. Es ist daher nicht auszuschliessen, dass sich bereits eine Reihe von «Fake-Ärztinnen» auf Meineimpfungen.ch angemeldet hat.

Darüber hinaus hat die Republik beim Registrierungsprozess eine weitere, beinahe schon peinliche Sicherheitslücke entdeckt. Will eine Hackerin keine Covid-Impfdaten verändern, sondern sie «nur» einsehen, kann sie sich das gefälschte Medizindiplom sparen und stattdessen die Passwort-Reset-Funktion nutzen. Damit erhält sie einen Zugang auf die Plattform, der zunächst stark eingeschränkt aussieht. Mit ein paar technischen Kniffen gelingt es aber, die Einschränkungen zu umgehen und Zugriff auf Impfausweise zu erhalten.

Ich will es genauer wissen: Wie funktioniert der Zugriff ohne validierten Account?

Bei der Registrierung erhält man als medizinische Fachperson das Passwort erst nach Validierung des Medizindiploms zugestellt. Es reicht jedoch, nur den ersten Schritt der Anmeldung als medizinische Fachperson zu durchlaufen, die darauffolgende E-Mail mit der Bitte um eine Dokumentenkopie zu ignorieren und stattdessen über die Passwort-Reset-Funktion («Passwort vergessen») für den noch nicht validierten Account ein Passwort zu setzen. Dadurch kann ein Hacker selbst ein Passwort setzen und erhält so den Zugriff auf Meineimpfungen.ch.

Wer sich damit einloggt, scheint auf den ersten Blick noch keinen Zugriff auf die Covid-Impfausweise zu haben, da die Account-Validierung aussteht. Es wird allerdings nur der entsprechende Menüpunkt nicht angezeigt. Wenn man die URL für den Impfausweis kennt, kann man diese direkt in die Adresszeile des Browsers eingeben und so auf den Impfausweis zugreifen. Hacker können ausserdem das Access-Token auslesen, mit dem sämtliche Zugriffe des Benutzers authentisiert (d. h. diesem Benutzer zugeordnet)

werden. Dieses Access-Token lässt sich auch bei einem noch nicht validierten Account für den automatisierten Zugriff auf sämtliche Covid-Impfdaten nutzen.

3. Hacker können Impfausweise einsehen

Schleust sich eine Angreiferin auf die beschriebene Weise in die Plattform ein, hat sie Zugriff auf eine grosse Menge an sensiblen Daten. Mittels des «übernommenen» Accounts kann sie sich mit der Suchfunktion einfach bedienen und auf sämtliche erfassten Impfdaten zugreifen.

Wenn die Hackerin «nur» den Covid-19-Impfstatus einer Privatperson wissen möchte, geht es sogar noch einfacher, indem sie sich den Impfausweis bestimmter Personen als PDF beschafft. Dazu braucht sie neben dem Access-Token (siehe Box «Wie funktioniert der Zugriff ohne validierten Account?») lediglich die numerische Identifikationsnummer (ID) des jeweiligen Patienten und muss diese an die URL (also die Internet-Adresszeile) anhängen.

Die ID eines Patienten herauszufinden, klingt nach einer schwer zu überwindenden Hürde. Doch bei Meineimpfungen.ch sind die Zahlen weder besonders komplex noch zufallsgeneriert. Die ID-Nummer ist bloss ein Zeitstempel – sie gibt den Zeitpunkt an, wann der Patientenaccount angelegt wurde.

Ausgehend davon, dass die meisten Schweizer Einwohnerinnen sich erst mit dem Start der Covid-Impfkampagne Anfang Jahr angemeldet haben, kann die Hackerin mittels eines kleinen Programms sämtliche seit 1. Januar 2021 möglichen IDs für Abfragen nach Impfausweisen verwenden. Viele davon werden nicht existieren und zu einem Fehler führen. Doch gemäss dem technischen Report des IT-Security-Teams wäre theoretisch alle 15 Minuten ein gültiger Impfausweis aufrufbar. Wenn die Abfragen portionenweise verteilt über Tage oder nur nachts erfolgen, dürfte dies den Systembetreibern von Meineimpfungen.ch – der IT-Firma Arpage – kaum auffallen.

Die Problematik einer öffentlich in der URL einsehbaren und einfach erratbaren ID hat die Republik, ebenfalls unter Beteiligung des IT-Security-Experten Sven Fassbender, bereits am Beispiel des Reservationsportals Lunchgate beschrieben. Doch Impfdaten sind weitaus sensibler als Restaurantbesuche, weil es sich um Gesundheitsinformationen handelt.

Bekannt ist, dass sich alle Bundesrätinnen impfen liessen. Wie erwähnt gelang es der Republik, die Konten der beiden Bundesrätinnen Viola Amherd und Ignazio Cassis zu eruieren. Sie hätte auch problemlos ihren Impfausweis öffnen sowie auf den verabreichten Impfstoff und weitere persönliche Gesundheitsdaten zugreifen können.

Ich will es genauer wissen: Wie sehen weitere mögliche Angriffsszenarien auf die Impfplattform aus?

a) Account-Übernahme durch Cross-Site-Scripting (XSS)

Bei Meineimpfungen.ch können Privatpersonen nach Anlegen ihres Kontos bisher erfolgte Impfungen erfassen und diese beim nächsten Arztbesuch validieren (bestätigen) lassen. Wie Recherchen der Republik zeigen,

überprüft, codiert und filtert die Plattform Meineimpfungen.ch die von den Privatpersonen gemachten Texteingaben nur unvollständig, sodass Angreifer insbesondere auch Programmcode eingeben können. Dieser Programmcode wird dann anschliessend ausgeführt, wenn der Arzt die Impfdaten aufruft. In Fachkreisen ist diese Art von Angriff als *Cross-Site-Scripting* bekannt.

Das für eine Angreiferin Interessante dabei: Der eingeschleuste Programmcode kann mit den Zugriffsrechten des gerade eingeloggten Arztes ausgeführt werden. Kurz: Eine Hackerin übernimmt den Account eines Arztes. Mit entsprechendem Wissen über die Funktionsweise der Applikation kann der Code problemlos so gestaltet werden, dass er spezifische, eigentlich nur Fachpersonen zugängliche Funktionen ausführen kann. Dazu gehören die Validierung oder die Invalidierung von Impfungen ebenso wie das Erfassen von Vorerkrankungen von Patientinnen, aber auch – für Angreifer besonders interessant – das Auslesen sämtlicher Gesundheitsdaten von Patientinnen eines Arztes oder das Eintragen einer Covid-Impfung. Gerade im Falle von impfstatusabhängigen Freiheiten könnte Letzteres schnell an Bedeutung gewinnen.

Ein XSS-Angriff bedingt, dass jemand (in diesem Fall die medizinische Fachperson) persönlich am Rechner eingeloggt ist und auf die manipulierten Daten zugreift. Um dies zu erreichen, kann eine Hackerin den Umstand ausnutzen, dass Ärzte per E-Mail informiert werden, wenn eine Patientin innerhalb von Meineimpfungen.ch eine Mitteilung hinterlässt. Wie bei anderen Phishing-Attacken auch kann die Hackerin diese E-Mail mit einem entsprechend modifizierten Link selbst schreiben und dem Arzt zustellen. Beim Klick auf den Link zeigt Meineimpfungen.ch im Browser den vorab manipulierten Inhalt an und führt den zugehörigen Code aus.

b) Account-Übernahme mittels «Passwort-Hack»

Bei einem Passwort-Reset erhält man einen Passwort-Reset-Link mit einer sechsstelligen Zeichenfolge (Token) per E-Mail zugestellt, mit der Meineimpfungen.ch das neue Passwort dem richtigen Account zuordnet. Sechsstellige Tokens sind zu wenig komplex, sie können mithilfe des Durchspielens sämtlicher Möglichkeiten innert nützlicher Frist erraten werden. Dazu löst die Hackerin für eine Reihe von Fachpersonal-Accounts den Passwort-Reset aus, lässt ein Programm laufen, das so lange Tokens ausprobiert, bis die Passwort-Änderung erfolgreich ist, und testet anschliessend, in welchen der Fachpersonal-Accounts sie sich mit dem neuen Passwort einloggen kann.

Stark erleichtert wird dies durch das Fehlen von 2FA (2-Faktor-Authentifizierung) bei Fachpersonen-Accounts (für normale Benutzer ist 2FA nicht nur möglich, sondern sogar stark empfohlen). Dies mag auf den ersten Blick überraschen, ist aber dadurch erklärbar, dass sich in medizinischen Praxen aus rein praktischen Gründen oft mehrere Praxisassistenten und Ärztinnen einen einzigen Benutzeraccount teilen und es daher fürs Log-in nicht so einfach ist, den 2FA-Code der richtigen Person zuzustellen.

Die Plattform wurde abgeschaltet

Der elektronische Impfausweis verstösst mehrfach gegen das (noch veraltete) Datenschutzgesetz (das revidierte ist erst ab 2022 in Kraft). Die Stiftung setzt zudem auf Infrastruktur von amerikanischen Big-Tech-Unternehmen. So werden für die Nutzung des MyCovidVac-Moduls Google-Dienste wie etwa die Google-Cloud verwendet.

Die Stiftung hat auf die gemeldeten Mängel reagiert. Die Plattform wurde gestern Montag vorübergehend deaktiviert. Sprecherin Nicole Bürki sagt

zur Republik: «Die beschriebenen Sicherheitsmängel waren uns bis gestern Sonntag nicht bekannt.» Man werde alle Befunde prüfen und eine spezialisierte Drittfirma mit weitergehenden Checks beauftragen.

Die Republik hat die gefundenen Missstände ausserdem dem eidgenössischen Datenschutzbeauftragten gemeldet. Das Informatik-Team des Edöb hat die Schwachstellen daraufhin verifiziert und bestätigt. Der Datenschutzbeauftragte Adrian Lobsiger hat am Montag ein Aufsichtsverfahren gegen die Stiftung Meineimpfungen.ch eingeleitet. Die Stiftung wird damit nun aufgefordert, sich detailliert zu den Sachverhalten zu äussern und auch darzulegen, wie die Betroffenen im Fall von Datendiebstahl informiert werden.

Grégoire Gogniat, der Sprecher des Bundesamts für Gesundheit, sagt auf Anfrage der Republik: «Das BAG hat die Stiftung sofort beauftragt, den Hinweisen nachzugehen und die Mängel zu beheben.» Das BAG scheint sich aufgrund der wachsenden Kritik zunehmend von der Stiftung zu distanzieren. So betonte Sprecher Gogniat, dass Meineimpfungen.ch kein nationales Impfregister sei und die Eintragung freiwillig. Es sei zudem offen, mit welcher Plattform man für den staatlichen Impfausweis zusammenarbeiten werde, so das BAG letzte Woche im «Tages-Anzeiger».

Dabei waren die Absichten bis vor kurzem ganz andere: In Antworten auf parlamentarische Vorstösse nennt der Bundesrat die bestehende Plattform Meineimpfungen.ch als valable Kandidatin für einen staatlichen Impfausweis. Laut einem vertraulichen Dokument von Dezember 2020 – das allerdings im Netz verfügbar ist – scheint die Zusammenarbeit zwischen dem BAG und Meineimpfungen.ch bereits besiegelt zu sein: «(...) Dokumentation des Impfaktes für das Impfmonitoring, sowie für das Erstellen eines Impfausweises zuhanden der geimpften Personen, hat sich das BAG entschieden, mit myCovidVac zusammen zu arbeiten.» Der Bund hat gemäss Recherchen der «SonntagsZeitung» bereits 2,15 Millionen Franken investiert und weitere 250’000 Franken in Aussicht gestellt.

Ganz andere Vorstellungen hat da jedoch das Parlament. Dieses möchte gemäss Artikel 6a des soeben angepassten Covid-19-Gesetz eine digitale Impfpasslösung, die fälschungssicher, international anerkannt, datenschutzkonform ist und lokale Überprüfungen ermöglicht.

Meineimpfungen.ch erfüllt diese Standards in keiner Weise.

Zu den Updates

Seit der Publikation dieses Beitrags haben wir zwei Updates veröffentlicht. Beim ersten ging es um nicht gelöschte Benutzerkonten, erzwungene Registrierungen und Falschinformationen der Betreiber: das Update zu den gravierenden Sicherheitsmängeln bei Meineimpfungen.ch. Beim zweiten wird eine wüste Posse rund um die Frage beschrieben, ob die Daten der Nutzerinnen gelöscht werden sollen.