Update

Wie das Debakel um den digitalen Impfpass schöngeredet wird

Nicht gelöschte Benutzerkonten, erzwungene Registrierungen und Falschinformationen der Betreiber: das Update zu den gravierenden Sicherheitsmängeln bei Meineimpfungen.ch.

Von Adrienne Fichter und Patrick Seemann, 30.03.2021

Vergangene Woche publizierte die Republik eine Recherche zur Plattform Meineimpfungen.ch. Die Erkenntnisse, die in Zusammenarbeit mit den IT-Sicherheitsexperten Sven Fassbender, Martin Tschirsich und André Zilch gewonnen wurden, führten dazu, dass der elektronische Impfausweis vom Netz genommen wurde. Die Schwachstellen waren so gravierend, dass der Eidgenössische Datenschutzbeauftragte ein Aufsichtsverfahren einleitete.

Zur Recherche

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

Für das Bundesamt für Gesundheit (BAG) ist die Angelegenheit äusserst unangenehm. Das Amt hat sich rasch von der Plattform distanziert – obwohl es offensichtlich mit ihr zusammengearbeitet und Förderbeiträge gesprochen hatte. Virginie Masserey, Leiterin der Sektion Infektionskontrolle beim BAG, ist zudem als Stiftungsrätin von Meineimpfungen.ch zurückgetreten. Und an Pressekonferenzen betonten BAG-Direktorin Anne Lévy und Bundesrat Alain Berset unisono: Wir tragen keine Mitverantwortung.

Im Widerspruch zu diesen Äusserungen zeigt sich:

- Der elektronische Impfpass ist viel stärker in die institutionellen Prozesse der Schweizer Impfkampagne integriert als gedacht.
- Das Datenchaos ist noch viel grösser als angenommen.
- Die Stiftung hat in einer Medienmitteilung versucht, die gravierenden Mängel kleinzureden – auch mit groben Falschaussagen.

Das Recherche-Update in drei Punkten:

1. Zwangsregistrierung von Ärztinnen

Im Spital Thurgau konnte sich das Fachpersonal im Frühjahr impfen lassen. Der elektronische Eintrag bei Meineimpfungen.ch war dabei für Ärztinnen obligatorisch, wie ein Dokument zeigt, das der Republik vorliegt. Eine Fachperson, die sich bei uns meldete, sagt, dass diese Zwangseintragung für grosse Irritation sorgte. Das Spital Thurgau reagierte nicht auf eine Anfrage.

Wie sehr das elektronische Impfbüchlein in den kantonalen Abläufen integriert ist, zeigte sich in den Tagen nach unserer Recherche. Der Hinweis und die Empfehlung zu Meineimpfungen.ch wurde etwa in St. Gallen oder in Zürich erst Tage später auf Webseiten und Formularen entfernt. In einigen Kantonen steht die Empfehlung noch heute auf dem Papier.

2. Daten trotz Löschungsbegehren immer noch vorhanden

Zwischenzeitlich haben wir zahlreiche Zuschriften von Betroffenen erhalten. Manche melden uns, dass ihre Benutzerkonten auf Meineimpfungen.ch trotz Löschungsbegehren immer noch existierten. Ein Leser schildert, wie er 2015 einen Antrag auf Löschung gestellt hat. Dies, nachdem er erfahren hatte, dass die ehemalige BAG-Datenbank an eine private Stiftung übertragen werde.

Die Stiftungsratspräsidentin Claire-Anne Siegrist bestätigte damals die Löschung des Benutzerkontos in einer E-Mail, die der Republik vorliegt. Doch letzte Woche erhielt der Leser die offizielle E-Mail, in der die Stiftung über die Sicherheitsmängel und über den Unterbruch der Plattform informierte. Das bedeutet: Sein Benutzerkonto wurde de facto gar nie gelöscht. Seine Impf- und Gesundheitsdaten lagen also seit sechs Jahren auf den Servern von Meineimpfungen.ch, ohne dass er davon wusste. Es handelt sich um einen weiteren groben Verstoss gegen das Datenschutzgesetz.

Sprecherin Nicole Bürki sagt dazu: «Daten von Nutzerinnen und Nutzern werden standardmässig nicht per sofort gelöscht, um eine Wiederherstellung zu ermöglichen. In der Datenschutzerklärung der Plattform wurde über diesen Umstand informiert.» Doch diese Erklärung ist fragwürdig: Erstens war die Datenschutzerklärung bis Januar 2021 – als die Republik die ersten technischen Schwachstellen publik gemacht hat – denkbar knapp gehalten. Die Notwendigkeit temporärer Datenspeicherungen war gar nicht erwähnt. Zweitens: Im vorliegenden Fall liegt der Löschungsantrag sechs Jahre zurück.

Die Stiftung stellte nun ebenfalls fest, dass sie jahrelang einen Datenfriedhof von vermeintlich gelöschten Konten gespeichert hat. Sprecherin Bürki räumt ein: «Bei der Überwachung des E-Mail-Versandes an alle Nutzerinnen und Nutzer der Plattform wurde festgestellt, dass die Daten einzelner Nutzerinnen und Nutzer noch nicht definitiv gelöscht waren. Diese Daten werden nun definitiv gelöscht, und es wird abgeklärt, wieso diese Daten noch nicht definitiv gelöscht waren.»

3. Irreführende Medienmitteilung

Die Stiftung Meineimpfungen.ch hat ihre Nutzerinnen erst vier Tage nach unserer Meldung und zwei Tage nach der Publikation unserer Recherche

über die Deaktivierung der Plattform informiert. Sie gab ausserdem am 26. März eine sonderbare Medienmitteilung heraus.

Darin betonte sie, dass alle Schwachstellen geschlossen seien und es keine Fälle von Missbrauch gebe: «Die seit Montagmorgen durchgefu⊠hrten Untersuchungen haben ergeben, dass keine Daten manipuliert, kompromittiert oder gestohlen wurden.»

Brisant ist die Medienmitteilung aus drei Gründen: erstens wegen irreführender Aussagen. Zweitens, weil sie existierende gravierende Mängel bewusst nicht erwähnt. Und drittens, weil sie auch faktisch falsch ist.

- **Zu den irreführenden Aussagen.** Die Stiftung schreibt etwa: «Eine unbefugte Registrierung als Fachperson mit vollem Zugriff wäre nur durch Vorlage eines gefälschten Arzt- oder Apothekerdiploms/-ausweises (...) möglich gewesen.» Die Beschwichtigung zu den gefälschten Ausweisen ist eine krasse Verharmlosung einer groben Schwachstelle. Denn eine Hackerin kann sich hier einiger Vorlagen im Internet bedienen.
- **Zu den nicht erwähnten Mängeln.** Die Stiftung erwähnt zwar mögliche XSS-/CSRF-Lücken (Cross-Site-Scripting-Attacken), jedoch nur im Zusammenhang mit gefakten Fachpersonenkonten, was eine Falschaussage ist. Denn dieses Angriffsszenario hat nichts mit der erwähnten Schwachstelle – dem mittels gefälschten Ausweises erschlichenen Fachpersonenkonto – zu tun. Im Gegenteil: Es kommt vor allem bei «echten» Fachpersonenkonten zum Zug. Etwa, wenn ein Hacker eine Nachricht mit eingeschleustem Programmcode an eine nichts ahnende Ärztin auf der Plattform Meineimpfungen.ch verschickt und damit ihr Konto fernsteuern kann. In der Medienmitteilung wird zudem kein Wort darüber verloren, dass Meineimpfungen.ch ein offenes Telefonbuch für alle registrierten Fachpersonen ist: Damit ist der Zugriff auf die Daten, Impfindikatoren und Impfdetails sämtlicher in der Schweiz bisher gegen Covid geimpften Personen gemeint. Hierbei handelt es sich um eine krasse konzeptionelle Schwäche, wie es im Fachjargon heisst.
- **Zu den faktischen Fehlern.** Die Medienmitteilung impliziert, dass sich die Fehler und Lücken primär im MyCovidVac-Modul befinden. Doch die von uns gefundenen XSS-/CSRF-Lücken wie auch die unsichere Fachpersonenregistrierung beziehen sich auf die gesamte Plattform Meineimpfungen.ch und damit auf alle eingetragenen Gesundheitsdaten.

Dass die Stiftung in der kurzen Zeit sämtliche Dateneinträge verifiziert und vermutlich seit Jahren existierende Sicherheitslücken geschlossen haben soll, ist fraglich. Nicht zuletzt, weil eine Ärztin theoretisch «legal» über ihr Fachpersonenkonto Daten aller 450’000 angemeldeten Personen absaugen konnte – ohne dass dies jemand von der Stiftung bemerkt hätte.

Dabei jeglichen Missbrauch von Daten nach vier Tagen Prüfung auszuschliessen, ist eine gewagte Aussage, die angezweifelt werden kann.