1 Zusammenfassung

Angesichts der geplanten Einführung eines EU-weiten Impfnachweises zur Überwindung der Reisebeschränkungen wurde die Sicherheit der vom BAG derzeit favorisierten Schweizer Umsetzung auf der Plattform *meineimpfungen.ch* und *services.mycovidvac.ch* der *Stiftung meineimpfungen* einer oberflächlichen, äusserlichen Betrachtung unterzogen. Im Rahmen dieses ehrenamtlichen Engagements wurden zahlreiche nachfolgend dokumentierte kritische Sicherheitsmängel identifiziert und am 21.03.2021 an die *Stiftung meineimpfungen* gemeldet.

Viele der identifizierten Sicherheitsmängeln fallen in die bekannten Kategorien der OWASP-Top-10[1]. Einige Sicherheitsmängel beziehen sich auf konzeptionelle und organisatorische Defizite. In Summe ermöglichen sie auch ungeübten Angreifern auf verschiedenen Wegen vollumfänglichen Zugriff auf die Daten von Patienten sowie Fachpersonen. Weder die Vertraulichkeit noch die Integrität oder Verfügbarkeit der hinterlegten Gesundheitsdaten ist gewährleistet.

Nachfolgend sind einige der kritischen Sicherheitsmängel gelistet:

- Ein Online-Brute-Force-Angriff auf die Passwort-Reset-Funktionalität ermöglicht Angreifern innerhalb kurzer Zeit einen Fachpersonen-Account zu übernehmen.

- Unter Ausnutzung von Sicherheitsmängeln im Registrierungsprozess können Unberechtigte einen neuen Fachpersonen-Account ohne Legitimationsprüfung anlegen.

- Auch die Legitimationsprüfung selbst kann aufgrund gravierender konzeptioneller Schwächen einfach überwunden werden.

- Aufgrund des fehlenden Berechtigungskonzepts können Angreifer in Besitz eines zuvor erlangten Fachpersonen-Accounts auf persönliche Informationen sowie die COVID-19-Impfnachweise aller registrierten Patienten zugreifen.

- Mit Hilfe sog. Cross-Site-Request-Forgery- und Cross-Site-Scripting-Angriffe können Unberechtigte zudem gezielt sowohl Fachpersonen- als auch Patienten-Accounts übernehmen und darüber weitere Gesundheitsdaten abrufen, darunter Angaben zu chronischen Erkrankungen, HIV-Infektionen und Krebsleiden.

Im nachfolgenden Report sind diese und weitere identifizierte Schwachstellen jeweils zusammen mit einer einfachen Risikoeinstufung und Massnahmen zu deren Behebung beschrieben.

Aus Zeitgründen konnten nicht alle oberflächlich beobachteten Sicherheitsmängel dokumentiert werden, darunter weitere Cross-Site-Scripting-Angriffsmöglichkeiten, unverschlüsselte Kommunikation beispielsweise zwischen Webanwendung und Identity-Provider des HIN, unsichere Kanäle wie SMS für den Passwort-Reset, Informationspreisgabe per Referrer-Leakage und viele mehr.

[1] https://owasp.org/www-project-top-ten/

In Anbetracht des hohen Schutzbedarfs der verarbeiteten Gesundheitsdaten müssen die betroffenen Dienste unverzüglich ausser Betrieb genommen werden. Es ist von einer vollständigen Kompromittierung der Webanwendung auszugehen. Die registrierten Patienten sind zu informieren. Den registrierten Fachpersonen ist das Vertrauen und somit der Zugriff zu entziehen, da seitens der Betreiber nicht zwischen legitimen und nicht-legitimen Accounts unterschieden werden kann. Aktuell ist die Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten Informationen nicht gewährleistet.

Vor einer Wiederinbetriebnahme der Webanwendung müssen alle Komponenten und Prozesse eine tiefgehende Prüfung durch eine qualifizierte Stelle durchlaufen. Es muss eine dem Schutzbedarf angemessene Registrierung und Legitimationsprüfung von Fachpersonen eingeführt und durchgesetzt werden. Erst nach der Behebung aller identifizierten Sicherheitsmängel ist ein weiterer Betrieb zu verantworten.

2 Übersicht der identifizierten Sicherheitsmängel

Titel	Risiko
Injektion von HTML-Code in E-Mails	**Mittel**
Fehlende Autorisierungsprüfung	**Hoch**
Passwort-Reset-Token von unzureichender Entropie	**Kritisch**
Aktivieren von Fachpersonen-Accounts ohne Legitimationsprüfung	**Kritisch**
Unzureichende Legitimationsprüfung von Fachpersonen	**Kritisch**
Fehlendes Berechtigungskonzept bei Zugriff auf Patienten durch Fachpersonen	**Kritisch**
Authentisierung von Fachpersonen auf unzureichendem Vertrauensniveau	**Hoch**
Cross-Site-Scripting	**Hoch**
Cross-Site-Request-Forgery	**Hoch**

3 Befunde

3.1 Injektion von HTML-Code in E-Mails

Betroffene Anwendung	meineimpfungen.ch
Klasse	Ausgabecodierung
Risiko	Mittel

Die Webanwendung ist für HTML-Injektionen in Mitteilungen zwischen Patienten und Fachpersonen anfällig. Die Erfolgswahrscheinlichkeit gezielter Phishing-Angriffe auf Fachpersonen steigt dadurch beträchtlich.

Ein Angreifer in der Rolle eines Patienten kann einer Fachperson - ohne deren Zutun - zunächst Zugriff auf das eigene Dossier gewähren und anschliessend Mitteilungen an diese Fachperson senden. Die Fachperson erhält dann eine HTML-E-Mail mit dem Inhalt der Mitteilung.

Fügt der Angreifer HTML-Code in die Mitteilung ein, wird dieser ohne angemessene Ausgabecodierung durch die Webanwendung unverändert in die HTML-E-Mail übernommen und bei Betrachten der E-Mail durch die Fachperson in deren E-Mail-Client entsprechend dargestellt.

Die E-Mail wird dabei im Namen von *meineimpfungen.ch* (no-reply@mesvaccins.ch) versendet. Aufgrund des vertrauenswürdigen Absenders ist ein gesteigertes Vertrauen der Fachperson in den authentisch erscheinenden Inhalt der E-Mail zu erwarten.

Diese Schwachstelle kann ausgenutzt werden, um beispielsweise Links oder Bilder in der E-Mail anzuzeigen. So kann der Angreifer die Fachperson auf eine eigene Webseite locken und sie zu der Eingabe von Login-Daten bewegen (Phishing) oder den im Befund 3.9 beschriebenen Angriff ausführen.

Empfehlung

Die systematische Untersuchung der Behandlung aller Benutzereingaben durch die Webanwendung wird empfohlen.

Die Webanwendung muss den E-Mail-Client davor bewahren, Benutzereingaben als potentiell missbräuchlichen HTML-Code zu interpretieren. Dies gelingt beispielsweise durch dem Ausgabekontext angemessene Ausgabecodierung. Beispielsweise dürfen Benutzereingaben, welche innerhalb eines HTML-Textnode ausgegeben werden, keine HTML-Steuerzeichen beinhalten - diese müssen in entsprechende HTML-Entities umgewandelt werden.

Korrekte Ausgabecodierung ist ausreichend, um die beschriebene HTML-Injektion zu verhindern. Alternativ kann auch gänzlich auf die Ausgabe der Mitteilung innerhalb einer E-Mail verzichtet werden.

3.2 Fehlende Autorisierungsprüfung

Betroffene Anwendung	meineimpfungen.ch
Klasse	Autorisierung
Risiko	Hoch

Die Webanwendung verzichtet teilweise auf eine Autorisierungsprüfung und erlaubt z. B. Angreifern in der Rolle eines Patienten den Zugriff auf und die Manipulation bestimmter Daten anderer Patienten.

Die Webanwendung prüft in einigen Fällen zwar, ob eine empfangene HTTP-Anfragen auch tatsächlich von einem eingeloggten bzw. authentisierten Benutzer stammt, nicht aber, ob der authentisierte Benutzer auch berechtigt bzw. autorisiert ist, eine solche HTTP-Anfrage auszuführen.

Während der Untersuchung wurde festgestellt, dass die Webanwendung bei der Ausführung folgender Aktionen auf eine Autorisierungsprüfung verzichtet:

- Hinterlegen von «ungewollten Impfungen» bei anderen Patienten
- Bearbeiten von fremden «Gruppen» (Communities)
- Zuordnung von fremden «Dossiers» zu der eigenen «Gruppe»

Zur Ausführung der vorgenannten Aktionen genügt es, eine HTTP-Anfrage von einem beliebigen authentisierten Benutzer abzusenden, dabei aber den Parameter *personId oder communityId* zu verändern, um die Aktionen im Kontext eines anderen Patienten auszuführen. So können beispielsweise ungewollte Impfungen bei einem anderen Patienten hinterlegt, die Namen von Gruppen anderer Patienten verändert und Dossiers anderer Patienten zu der eigenen Gruppe hinzugefügt werden.

Im folgenden Beispiel kann eine beliebige existierende *communityId* eines anderen Patienten eingegeben werden, um diese anschliessend zu manipulieren:

```
https://www.meineimpfungen.ch/community-edit.html?communityId=●●●●●●●●●●
```

Auszug 1 – Die URL zum Bearbeiten einer Gruppe, identifiziert über den HTTP-GET-Parameter "communityId"

Insbesondere das Hinterlegen von ungewollten Impfungen für andere Patienten birgt ein Gefahrenpotential. Abhängig davon, wie eine Fachperson diese Information verarbeitet, könnte es dazu führen, dass ein Patient eine aus medizinischer Sicht notwendige Mitteilung über eine Impfung nicht erhält.

Um diesen Angriff auszuführen, muss der Angreifer die *patientId* oder *communityId* der Zielperson kennen oder erraten (siehe auch Befund 3.6).

Empfehlung

Alle Anfragen müssen serverseitig vor der Weiterverarbeitung einer Berechtigungs- bzw. Autorisierungsprüfung unterzogen werden. Dies gilt sowohl für den horizontalen Kontext (Zugriff auf Accounts mit gleicher Rolle, Patient-Patient), wie auch für die Rollen untereinander (Patient-Fachperson, Privilege-Escalation). Bei der Vergabe von Berechtigungen sollte dem Least-Privilege-Prinzip[2] gefolgt werden.

[2] https://us-cert.cisa.gov/bsi/articles/knowledge/principles/least-privilege

3.3 Passwort-Reset-Token von unzureichender Entropie

Betroffene Anwendung	meineimpfungen.ch
Klasse	Authentisierung
Risiko	Kritisch

Angreifer können durch Erraten eines von der Webanwendung per E-Mail oder SMS an den Benutzer verschickten Passwort-Reset-Tokens dessen Passwort ändern und damit insbesondere den Account einer Fachpersonen übernehmen.

Die Webanwendung bietet jedermann die Möglichkeit, unter Kenntnis von Telefonnummer oder E-Mail-Adresse (Patient) bzw. EAN oder GLN (Fachperson) das Passwort eines Benutzer-Accounts zurückzusetzen (Passwort-Reset).

Im Fall einer Fachperson wird der Passwort-Reset mit der Eingabe der entsprechenden EAN bzw. GLN gestartet. Nun erhält der Account-Inhaber eine E-Mail-Benachrichtigung mit einem Hyperlink. Dieser beinhaltet ein Passwort-Reset-Token und hat das folgende Format:

```
https://www.meineimpfungen.ch/passwort-reset.do?token=●●●●●●&usertype=SPECIALIST
```

Auszug 2 – Die URL in der Passwort-Reset-E-Mail enthält das sechsstelliges Reset-Token.

Das Reset-Token im Query-Parameters *token* setzt sich aus lediglich sechs alphanumerischen Zeichen in Gross- und Kleinschreibung zusammen. Dies entspricht 62^6 möglichen gültigen Token. Fordert ein Angreifer nun beispielsweise für alle derzeit registrierten 11.000 Fachpersonen-Accounts ein Reset-Token an, so liegt die Wahrscheinlichkeit, dass ein einziges zufällig geratenes Token zu einem der 11.000 Fachpersonen-Accounts gehört, bei knapp 0.00002 %. Mit systematischem Durchprobieren aller möglichen Token innerhalb eines Online-Brute-Force-Angriffes mit realistischen 500 Anfragen pro Sekunde ist ein Erfolg, also das Erraten eines Reset-Tokens eines zufälligen Fachpersonen-Accounts, in etwa zwei Stunden zu erwarten.

Im Gegensatz zu Patienten haben Fachpersonen, welche nicht den HIN-Login nutzen, keine Möglichkeit, ihren Account durch Aktivieren einer Zwei-Faktor-Authentisierung zu schützen.

Die EAN bzw. GLN der registrierten Fachpersonen können der öffentlichen, lizenzfreien *Partnerrefdatabase* der *Stiftung Refdata* unter *https://refdata.ch* entnommen werden.

Empfehlung

Es wird empfohlen, eine dem Stand der Technik entsprechende, sichere Zwei-Faktor-Authentisierung für alle Benutzer verbindlich zu implementieren. Solange weiterhin Passwort-Reset-Token zum Einsatz kommen (siehe Befund 3.7), sollten diese von ausreichender Entropie sein, um einen Online-Brute-Force-Angriff für einen Angreifer unattraktiv zu machen.

3.4 Aktivieren von Fachpersonen-Accounts ohne Legitimationsprüfung

Betroffene Anwendung	meineimpfungen.ch
Klasse	Registrierung
Risiko	Kritisch

Die Webanwendung gibt Fachpersonen weitreichende Privilegien. Daher müssen sich diese nach Registrierung einer Legitimationsprüfung unterziehen, diese kann jedoch vollständig umgangen werden. Unberechtigte gelangen darüber an Fachpersonen-Accounts und können auf Patientendaten zugreifen.

Die Webanwendung erlaubt jedermann die Registrierung eines Accounts sowohl in der Rolle eines Patienten als auch einer Fachperson. Gegenüber Patienten, welche lediglich auf selbst eingetragene Daten zugreifen können, verfügen Fachpersonen über weitreichende Berechtigungen (siehe Befund 3.6). Daher ist vor Aktivierung des Accounts einer Fachperson deren Identität sowie deren fachliche Qualifikation sicher zu prüfen.

Die Registrierung einer Fachperson erfolgt nach vorheriger Eingabe einer EAN bzw. GLN über folgendes Webformular:

Abbildung 1 - Screenshot der Eingabe-Maske zur Registrierung von Fachpersonen

Die EAN bzw. GLN einer real existierender Fachpersonen kann der öffentlichen, lizenzfreien *Partnerrefdatabase* der *Stiftung Refdata* unter *https://refdata.ch* entnommen werden. Nicht registrierte und somit noch verfügbare EAN bzw. GLN können ausserdem als angemeldeter Patient eingesehen werden:

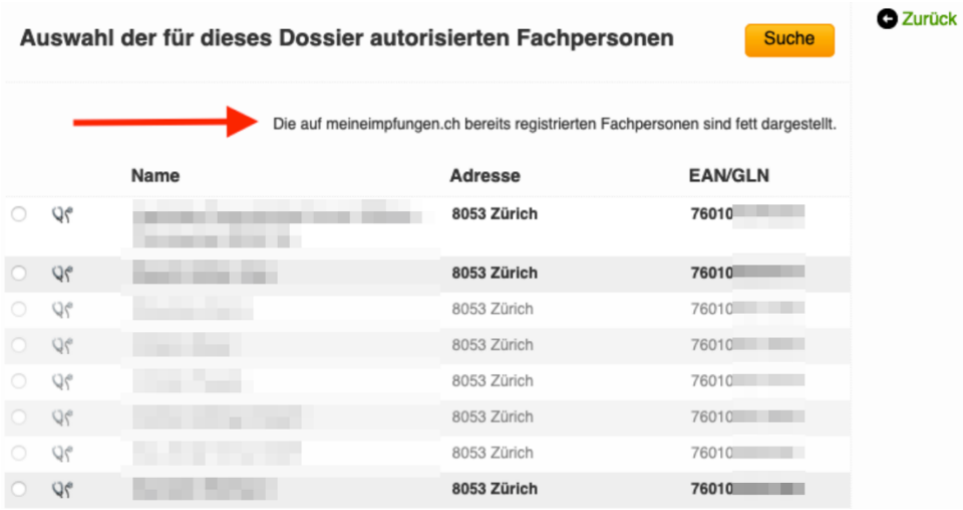

Abbildung 2 - Auszug aus der Patienten-Ansicht zur Auswahl einer Fachperson für die Dossier-Freigabe

Nach dem Absenden des Webformulars startet für die Fachperson der «manuelle Validierungsprozess». Diese Legitimationsprüfung soll sicherstellen, dass lediglich Ärzte oder Apotheker, deren Ausbildung das Gebiet der Immunisierung umfasst, einen Zugriff erhalten.

Es hat sich jedoch herausgestellt, dass es möglich ist, diesen «manuellen Validierungsprozess» zu umgehen. Hierzu wird direkt nach Absenden des obigen Webformulars unter der angegebenen EAN bzw. GLN ein Passwort-Reset angefordert. Kurz darauf wird ein gültiges Passwort-Reset-Token an die angegebene E-Mail-Adresse gesendet. Damit kann ein initiales Passwort gesetzt werden.

Anschliessend ist mit EAN bzw. GLN und dem gesetzten Passwort ein Login als Fachperson möglich. Die eingeloggte Fachperson kann dann unter der URL *https://www.meineimpfungen.ch/specialist-covid-vac-flow.do* ein Access-Token zur Authentisierung an dem Dienst *services.mycovidvac.ch* abrufen:

```
<specialist-covid-app
                    accessToken="●●●●●●●●●●"
                    patientId=""
                    covidApiBaseUrl="https://services.mycovidvac.ch"
                    language="de">
</specialist-covid-app>
```

Auszug 3 - accessToken Wert enthalten in der HTTP-Antwort

Anschliessend kann die API dieses Dienstes genutzt werden, um beispielsweise vorhandene COVID-19-Impfnachweise abzurufen. Hierzu ist neben dem obigen Access-Token im Authorization-Header eine *patientId* im HTTP-Query-Parameter mitzusenden:

```
GET /api/v1/vaccination-card/?patientId=●●●●●●●●● HTTP/1.1
Host: services.mycovidvac.ch
User-Agent: ●●●●●●●●●●
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.meineimpfungen.ch/
Authorization: Bearer ●●●●●●●●●●
Origin: https://www.meineimpfungen.ch
DNT: 1
Connection: close
```

```
Content-Length: 114
```

Auszug 4 - HTTP-GET-Anfrage zum Herunterladen eines COVID-19-Impfnachweises

Abbildung 3 - Screenshot eines COVID-19-Impfnachweises

Der Wert des Parameters *patientId* stellt einen 16-stelliger Unix-Zeitstempel dar und gibt auf die Mikrosekunde genau den Registrierungs-Zeitpunkt des zugehörigen Patienten an. Ist einem Angreifer keine gültige *patientId* bekannt, führt ein Online-Brute-Force-Angriff zum Erfolgt: Unter realistischen Annahmen über die Anzahl der innerhalb eines Zeitraums registrierten Patienten und bei realistischen 1.000 Anfragen pro Sekunde (Google-Cloud-Infrastruktur) kann alle ca. 15 Minuten ein Impfnachweis abgerufen werden.

Empfehlung

Accounts von Fachpersonen dürfen erst nach erfolgreich durchlaufener Legitimationsprüfung für den Zugriff auf die Webanwendung autorisiert werden (siehe hierzu Befund 3.5).

3.5 Unzureichende Legitimationsprüfung von Fachpersonen

Betroffene Anwendung	meineimpfungen.ch
Klasse	Registrierung
Risiko	Kritisch

Die Webanwendung gibt Fachpersonen weitreichende Privilegien. Daher müssen sich diese nach Registrierung einer Legitimationsprüfung unterziehen, diese erfolgt jedoch allein auf Grundlage eingereichter Fotos einer Health Professional Card (HPC), eines Diploms oder Fachausweises. Unberechtigte gelangen darüber an Fachpersonen-Accounts und können auf Patientendaten zugreifen.

Die Webanwendung erlaubt jedermann die Registrierung eines Accounts sowohl in der Rolle eines Patienten oder einer Fachperson. Gegenüber Patienten, welche lediglich auf selbst eingetragene Daten zugreifen können, verfügen Fachpersonen über weitreichende Berechtigungen (siehe Befund 3.6). Daher ist vor Aktivierung des Accounts einer Fachperson deren Identität sowie deren fachliche Qualifikation sicher zu prüfen.

Die Fachperson durchläuft dabei einen «manuellen Validierungsprozess», zu dessen Beginn von einer Mitarbeiterin der *Stiftung meineimpfungen* per E-Mail das Foto einer Health Professional Card (HPC), eines Diploms oder Fachausweises angefordert wird.

Der folgende Auszug zeigt die entsprechende Passage in einer von der *Stiftung meineimpfungen* gesendeten E-Mail:

> *… Als Stiftung sind wir verpflichtet, die Fachpersonenprofile unter der Verantwortung von Ärzten und Apothekern, deren Ausbildung das Gebiet der Immunisierung umfasst zu überprüfen.*
>
> *Könnten Sie uns bitte noch ein Foto von Ihrer Health Professional Card (HPC), Ihr Diplom / Fachausweis mailen, damit wir Ihnen den Zugriff erteilen können? …*

Es liegt auf der Hand, dass diese Art der Legitimationsprüfung keine Identitätsfeststellung des Account-Inhabers bzw. des Inhabers des Authentisierungsmittels zulässt. Selbst bei Einreichen einer unverfälschten Fotokopie der geforderten Dokumente fehlt die Bindung an den tatsächlichen Account-Inhaber.

Zudem kann zwar gemäss Art. 180 ZPO eine Urkunde in Kopie eingereicht werden, jedoch führt dies immer zu einem Verlust des Beweiswerts, wenn anhand der physischen Beschaffenheit des Originals Beweis geführt werden muss.[3] Der «manuelle Validierungsprozess» stellt zu keinem Zeitpunkt sicher, dass zu der eingesandten Fotokopie überhaupt ein Original existiert. Ein nachträgliches Einreichen «im Bedarfsfall» scheidet grundsätzlich aus, da aufgrund des hohen Schutzbedarfs der Patientendaten von Anfang an sichergestellt sein muss, dass nur Berechtigte überhaupt einen Zugang erlangen können. Die Prüfung einer Fotokopie ist gemäss Schweizer Bundesgericht nicht ausreichend, um eine positive Urheberschaftsaussage über ein Dokument zu treffen.

[3] Elektronische Aktenführung: Beweisführung mit eingescannten Dokumenten; Lukas Fässler, Zug, 4.8.2014

Wörtlich sagt das Schweizer Bundesgericht[4] dazu:

> *Bei Nicht-Originalen bestehen elementare Informationsdefizite in den Merkmalen der Strichbeschaffenheit, Druckgebung, des Bewegungsflusses und der Bewegungsrichtung, deren Analyse und übereinstimmende Merkmalsausprägung für eine positive Urheberschaftsaussage unverzichtbar sind. Die Erkenntnismöglichkeiten bei der Begutachtung von Nicht-Originalen beschränken sich daher auf eine "Tendenzaussage" (zum Ganzen: Umgang mit Nicht-Originalen in der Forensischen Handschriftenuntersuchung, Richtlinie 4.00 der Gesellschaft für Forensische Schriftuntersuchung [http://www.gfs2000.de]).*

Im weiteren Verlauf:

> *Es ist allgemein anerkannt, dass nur die am Original erhobenen Befunde eine positive Urheberschaftsaussage begründen können und der Nachweis der Echtheit einer Fotokopie nicht möglich ist. Nicht-Originale enthalten lediglich bildliche Darstellungen von Schreibleistungen und es existieren keine hinreichend sicheren Methoden nachzuweisen, dass die darin enthaltenen Schriftzüge unverändert und vollständig reproduziert worden sind. Es muss deshalb bereits offenbleiben, ob ein entsprechendes Original überhaupt jemals in der dargestellten Form existiert hat.*

Der Zugang zur Webanwendung kann alternativ auch mittels *myFMH eID* erfolgen. Auch das von der FMH beschriebene Verfahren[5] zum Erlangen der *myFMH eID* bietet hier keine hinreichende Sicherheit:

> *Zur Registrierung für myFMH eID basic ist eine Kopie des gültigen Reisepasses oder der gültigen Identitätskarte erforderlich (Vorder- und Rückseite).*

Ähnliches gilt für die verschiedenen Ausgestaltungen der ebenfalls zulässigen *HIN eID*. Für bisher registrierte und aktivierte Fachpersonen-Accounts muss daher die Vermutung gelten, dass die zugehörigen Authentisierungsmittel in die Hände von Unberechtigten gelangt sein können. Die *Stiftung meineimpfungen* kann ohne erneute sichere Legitimationsprüfung nicht zwischen legitimen und nicht-legitimen Fachpersonen-Accounts unterscheiden.

Empfehlung

Fachpersonen müssen sicher und rechtskonform registriert werden. Hierzu sind die Schritte Identitätsfeststellung, Prüfung der fachlichen Qualifikation sowie Ausgabe der Authentisierungsmittel auf hohem Vertrauensniveau gemäss Stand der Technik zu durchlaufen.

Bis zu einer sicheren Verifizierung der Fachpersonen-Accounts ist diesen das Vertrauen und somit auch der Zugang zu der Webanwendung zu entziehen.

[4] https://www.bger.ch/ext/eurospider/live/de/php/aza/http/index.php?highlight_docid=aza%3A%2F%2F31-08-2015-9C_634-2014&lang=de&type=show_document&zoom=YES&

[5] https://www.fmh.ch/dienstleistungen/mitgliedschaft/eid-myfmh.cfm#i144907

3.6 Fehlendes Berechtigungskonzept bei Zugriff auf Patienten durch Fachpersonen

Betroffene Anwendung	services.mycovidvac.ch
Klasse	Autorisierung
Risiko	Kritisch

Die Webanwendung erlaubt jeder der mehr als 11.000 registrierten Fachpersonen Zugriff auf Gesundheitsinformationen aller registrierten Patienten. Der Schaden im Fall einer Kompromittierung eines einzelnen Fachpersonen-Accounts ist unverhältnismässig hoch.

Registrierte Fachpersonen können über eine unter *services.mycovidvac.ch* bereitgestellte Suchfunktion uneingeschränkt auf die folgenden personenbezogenen Daten aller in der Webanwendung registrierten Patienten zugreifen:

- Vorname
- Nachname
- Geburtsdatum
- Geschlecht
- Adresse
- Versichertennummer
- Versicherungskasse
- Ausweisdetails
- E-Mail-Adresse
- Mobil-/Festnetznummer

Ausserdem können, falls bereits erfasst, die folgenden Informationen zu COVID-19 relevanten Vorerkrankungen und Werten eingesehen werden:

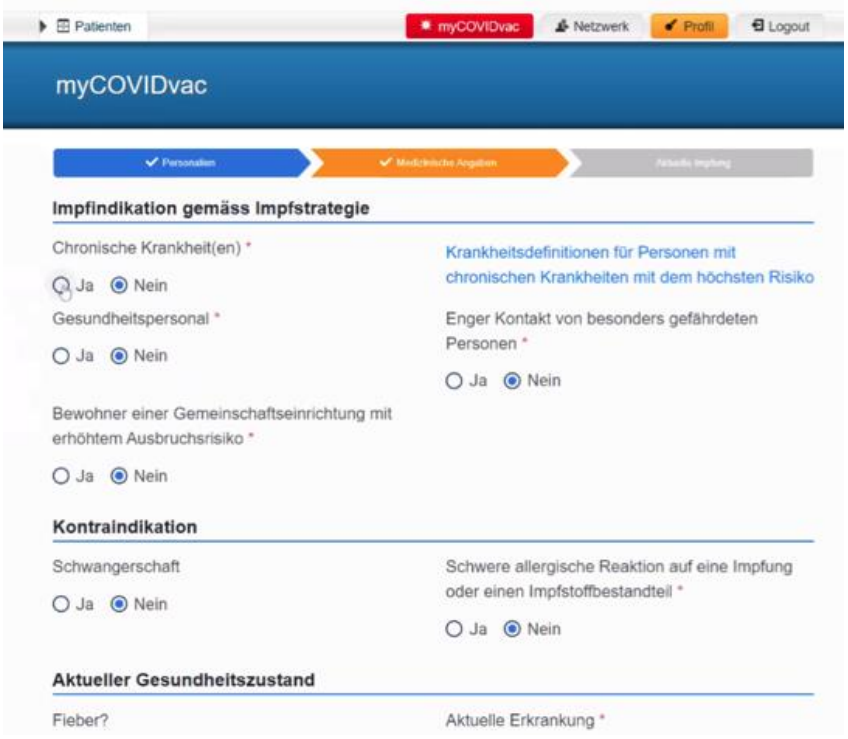

Abbildung 4 - Screenshot der erfassten medizinischen Angaben eines Patienten

Schlussendlich kann, sofern der Patient bereits gegen COVID-19 geimpft wurde, auch dessen COVID-19-Impfnachweis abgerufen werden. Nachdem ein Patient beide vorgeschriebenen COVID-19 Impfdosen erhalten hat. Wird ein sogenannter COVID-19-Impfnachweis erzeugt. Dieser enthält die folgenden Informationen in englischer Sprache und in Form eines QR-Codes:

- Name
- Vorname
- Geburtsdatum
- Geschlecht
- Pass-Nummer (falls angegeben)
- Impfstoff
- Datum der Impfung
- Name der Verabreichenden
- Lot-Nummer
- Signierte Informationen in Form eines QR-Codes zur «elektronischen Verifizierung»

Dadurch, dass jede Fachperson für den Zugriff auf jeden Patienten berechtigt ist bzw. von vornherein auf eine Berechtigungsprüfung verzichtet wird, entsteht im Fall der Kompromittierung eines einzigen Fachpersonen-Accounts (siehe dazu Befunde 3.4, 3.5) ein unverhältnismässig hoher Schaden. Denn die abrufbaren Daten lassen weitreichende Rückschlüsse auf den körperlichen Gesundheitszustand registrierter Patienten zu. Beispielsweise lässt sich allein anhand des Impfzeitpunkts ermitteln, ob der Geimpfte einer Prioritätengruppe angehört und daher ein sehr hohes Risiko für einen schweren oder tödlichen Krankheitsverlauf nach einer Infektion mit dem Coronavirus trägt.

Empfehlung

Der Zugriff auf Patientendaten durch Fachpersonen ist durch ein dem Risiko der Verarbeitung angemessenes Berechtigungskonzept einzuschränken. Fachpersonen sollten nur auf Informationen zugreifen können, nachdem dies durch den betroffenen Patienten autorisiert wurde.

3.7 Authentisierung von Fachpersonen auf unzureichendem Vertrauensniveau

Betroffene Anwendung	meineimpfungen.ch
Klasse	Authentisierung
Risiko	Hoch

Fachpersonen, die einen Account ohne HIN-Anschluss oder myFMH eID registriert haben, können keine Zwei-Faktor-Authentisierung (2FA) nutzen. Eine allein passwortbasierte Authentisierung auf niedrigem Vertrauensniveau ist angesichts des hohen Schutzbedarfs jedoch nicht ausreichend.

Eine Authentisierung mittels Passworts alleine erreicht lediglich ein niedriges Vertrauensniveau. Zugang zu Gesundheitsdaten erfordert jedoch nach den anerkannten Regeln der Technik, wie sie beispielsweise aus ISO/IEC 29115:2017 hervorgehen, mindestens auf einem hohen Vertrauensniveau.

Eine dem Stand der Technik entsprechende Authentisierung auf hohem Vertrauensniveau bedingt eine Zwei-Faktor-Authentisierung. Hierbei wird neben dem Passwort, einem sog. Wissensfaktor, auf einen weiteren sog. Besitzfaktor oder Biometrie gesetzt. Beide Faktoren können nicht auf demselben Weg angegriffen werden, beispielsweise durch Diebstahl, und gewähren somit ein deutlich höheres Vertrauen in die Echtheit der behaupteten Identität des Benutzers.

Dem Schutzbedarf der Webanwendung entsprechend muss insbesondere die Verwendung eines Fachpersonen-Accounts eine solche zusätzliche Authentifizierung voraussetzen. Die Verwendung eines solchen Accounts darf ohne 2-Faktor-Authentifizierung nicht möglich sein.

Empfehlung

Fachpersonen müssen sich auf mindestens hohem Vertrauensniveau mittels einer dem Stand der Technik entsprechenden, sichere Zwei-Faktor-Authentisierung authentisieren. Auch die weiteren Prozesse wie Ausgabe der Authentisierungsmittel, Passwort-Reset bzw. Wiederherstellung (siehe dazu auch Befund 3.3, 3.5) und Sperrung sind auf entsprechendem Vertrauensniveau umzusetzen.

3.8 Cross-Site-Scripting

Betroffene Anwendung	meineimpfungen.ch
Klasse	XSS
Risiko	Hoch

Die Webanwendung verzichtet auf eine angemessene Ausgabecodierung von Benutzereingaben und ermöglicht Angreifern das Einschleusen von clientseitig ausgeführtem JavaScript-Code (XSS). Dadurch können Accounts anderer Benutzer (insb. Fachpersonen) übernommen werden.

Eine Cross-Site-Scripting-Schwachstelle (XSS) erlaubt einem Angreifer das Einschleusen von schädlichem JavaScript-Code in den clientseitig interpretierten HTML-Code der Webanwendung. Der JavaScript-Code wird anschliessend im Browser des Benutzers ausgeführt und kann in dessen Namen und mit dessen Rechten mit der Webanwendung interagieren, ohne dabei die Same-Origin-Policy zu verletzen. Übliche Angriffsszenarien sind Phishing und Session-Hijacking.

Bei einer sog. Stored-XSS-Schwachstelle ist der JavaScript-Code durch den Angreifer serverseitig hinterlegt und wird bei Abrufen bestimmter Inhalte der Webanwendung an den Browser des Benutzers ausgeliefert und dort ausgeführt, ohne dass es einer direkten Interaktion zwischen Angreifer und Benutzer bedarf.

In verschiedenen Bereichen der Webanwendung wurden potentielle XSS-Schwachstellen identifiziert, von denen aus Zeitgründen allein die nachfolgend beschriebene Stored-XSS-Schwachstelle im Impfausweis eines Patienten im Test validiert wurde. Die Schwachstelle kann ausgenutzt werden, um eine eingeloggte Fachperson anzugreifen und deren Account zu übernehmen.

Hierzu erstellt der Angreifer ein Patienten-Profil mit einem manipulierten Impfausweis, welcher neben Impfdaten auch eingeschleusten JavaScript-Code beinhaltet. Anschliessend wird der anzugreifenden Fachperson, entsprechend dem vom System vorgeschlagenen Ablauf, Zugriff auf den manipulierten Impfausweis erteilt, verbunden mit der Bitte um Validierung. Sobald die Fachperson den Impfausweis öffnet wird der eingeschleuste JavaScript-Code in deren Browser ausgeführt.

Mit folgender HTTP-POST-Anfrage wurde JavaScript-Code in den Impfausweis eines authentisierten Patienten in der Rolle des Angreifers eingeschleust:

```
POST /vaccinations-edit.html HTTP/1.1
Host: www.meineimpfungen.ch
Connection: close
Content-Length: 577
Cache-Control: max-age=0
sec-ch-ua: ●●●●●●●●●●
sec-ch-ua-mobile: ?0
Upgrade-Insecure-Requests: 1
Origin: https://www.meineimpfungen.ch
Content-Type: application/x-www-form-urlencoded
User-Agent: ●●●●●●●●●●
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicatio
n/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
```

```
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://www.meineimpfungen.ch/
Accept-Encoding: gzip, deflate
Accept-Language: de-DE,de;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: ●●●●●●●●●

org.apache.struts.taglib.html.TOKEN=●●●●●●●●●&_csrf=
●●●●●●●●●&vaccinationId%281%29=●●●●●●●●●&vaccinationDate%281%29=
●●●●●●●●●&vaccineId%281%29=151&lot%281%29=
●●●●●●●●●%3Cb%3E3%3C%2Fb%3E&appliedBy%281%29=
●●●●●●●●●&validatedBy%281%29=&vaccinationDate%282%29=
●●●●●●●●●&vaccineId%282%29=76&lot%282%29=%3Cscript%3Ealert%28%27Verify+Me%27%
29%3C%2Fscript%3E&appliedBy%282%29=
●●●●●●●●●&validatedBy%282%29=&vaccinationDate%283%29=&vaccineId%283%29●●●●●
●●●●&lot%283%29=&appliedBy%283%29=&validatedBy%283%29=&personId=
●●●●●●●●●&submitted=true
```

Auszug 5 - HTTP-POST-Anfrage zum Speichern von JavaScript-Code in einem Freitextfeld des Impfausweises.

Wird der Impfausweis durch eine Fachperson geöffnet, liefert die Webanwendung den eingeschleusten JavaScript-Code in der HTTP-Antwort an deren Browser, wo er anschliessend ausgeführt wird:

```
HTTP/1.1 200 200
Date: ●●●●●●●●●
Server: Apache
Strict-Transport-Security: max-age=31536000; includeSubDomains
Pragma: No-cache
Cache-Control: no-cache,no-store,max-age=0
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Security-Policy: default-src 'self' repo.arpage.ch www.youtube.com themes.googleusercontent.com
services.mycovidvac.ch www.myvaccines.ch; script-src 'self' 'unsafe-inline' 'unsafe-eval' ssl.google-
analytics.com repo.arpage.ch; object-src 'self'; style-src 'self' 'unsafe-inline'; img-src 'self' data: repo.arpage.ch;
report-uri /report-service/csp-report
X-Permitted-Cross-Domain-Policies: master-only
Referrer-Policy: strict-origin
Content-Length: 328820
Connection: close
Content-Type: text/html;charset=UTF-8

…
<input type="text" name="vaccineName(6)" maxlength="100"
value="&lt;script&gt;alert(&quot;Verify+Me&quot;)&lt;/script&gt;" style="width: 100px;" class="text ui-
widget-content ui-corner-all">
…
```

Auszug 6 – Die HTTP-Antwort enthält zuvor eingeschleusten JavaScript-Code, dieser wird im Browser ausgeführt.

Je nach eingeschleustem JavaScript-Code kann der Angreifer beispielsweise die E-Mail-Adresse des Fachpersonen-Accounts ändern und diesen anschliessend durch einen Passwort-Reset übernehmen.

Empfehlung

Die systematische Untersuchung der Behandlung aller Benutzereingaben durch die Webanwendung wird empfohlen.

Die Webanwendung muss den Browser davor bewahren, potenziell gefährliche Benutzereingaben als HTML-, CSS- oder JavaScript-Code zu interpretieren. Dies gelingt beispielsweise durch dem Ausgabekontext angemessene Ausgabecodierung. So dürfen Benutzereingaben, welche innerhalb eines HTML-Textnode ausgegeben werden, keine HTML-Steuerzeichen beinhalten - diese müssen in entsprechende HTML-Entities umgewandelt werden.

Korrekte Ausgabecodierung ist ausreichend, um XSS zu verhindern. Eingabevalidierung kann jedoch als zusätzliche Schutzmassnahme implementiert werden[6]. Häufig lassen sich Benutzereingaben auf bestimmte Zeichenklassen einschränken, beispielsweise auf alphanumerische Zeichen.

Als zusätzliche Verteidigungsmassnahme sollte eine restriktive Content-Security-Policy (CSP) gesetzt werden, wodurch viele XSS-Angriffsvektoren von vornherein eliminiert werden können.

[6] https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

3.9 Cross-Site-Request-Forgery

Betroffene Anwendung	meineimpfungen.ch
Klasse	CSRF
Risiko	Hoch

Ein Angreifer kann über eine sog. Cross-Site-Request-Forgery (CSRF) im Namen und mit den Rechten eines angemeldeten Benutzers mit der Webanwendung interagieren. Dadurch können Accounts anderer Benutzer (insb. Fachpersonen) übernommen werden.

Die Webanwendung authentifiziert eingeloggte Benutzer anhand eines Session-Cookies (JSESSIONID) ohne «SameSite»-Attribut. Wird das «SameSite»-Attribut nicht gesetzt ist der Standard-Wert *lax*. Dieser Wert ist hat keine Auswirkung auf die im folgenden beschriebenen CSRF-Angriffe.

```
HTTP/1.1 302 302
Date: ●●●●●●●●●●
Server: Apache
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=●●●●●●●●●●; Path=/; Secure; HttpOnly
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-Frame-Options: SAMEORIGIN
Location: /community-list.html
Content-Length: 0
Content-Security-Policy: default-src 'self' repo.arpage.ch www.youtube.com themes.googleusercontent.com
services.mycovidvac.ch www.myvaccines.ch; script-src 'self' 'unsafe-inline' 'unsafe-eval' ssl.google-
analytics.com repo.arpage.ch; object-src 'self'; style-src 'self' 'unsafe-inline'; img-src 'self' data: repo.arpage.ch;
report-uri /report-service/csp-report
X-Permitted-Cross-Domain-Policies: master-only
Referrer-Policy: strict-origin
Connection: close
```

Auszug 7 – Die HTTP-Antwort nach erfolgreichem Login per HTTP-Header "Set-Cookie" ohne das Attribut "SameSite".

Der Browser sendet das Session-Cookie mit jeder HTTP-Anfrage an die Webanwendung, selbst wenn die Anfrage von einer anderen Seite stammt (Cross-Site-Request). Die Same-Origin-Policy hindert den Angreifer lediglich am Zugriff auf die HTTP-Antwort der Webanwendung, nicht jedoch am Absenden der HTTP-Anfrage im Namen des Benutzers.

Ein Angreifer kann diese Schwachstelle nur ausnutzen, indem er den Browser eines eingeloggten Benutzers dazu bringen kann, eine HTTP-Anfrage an die Webanwendung abzusenden. Dies gelingt beispielsweise, indem der Angreifer den Benutzer dazu bringen kann, einem präparierten Link aus einer E-Mail zu folgen. Auf diese Weise können allerdings nur HTTP-GET-Anfragen abgesendet werden, deren Schadpotential üblicherweise gering ist (Idempotenz). Gelingt es einem Angreifer jedoch, den Benutzer auf eine präparierte Webseite zu leiten oder ein präpariertes HTML-Dokument zu öffnen, können auch HTTP-POST-Anfrage an die Webanwendung gesendet werden - beispielsweise durch automatisiertes Absenden eines HTML-Formulars (siehe hierzu den Befund 3.3).

Tatsächlich verwendet die Webanwendung sog. CSRF-Token, um derartige CSRF-Angriffe zu vermeiden - jedoch nur bei HTTP-POST-Anfragen. Im Test liessen sich aber viele HTTP-

POST-Anfragen ohne Einschränkung auch als HTTP-GET-Anfrage senden. Damit ist die implementierte CSRF-Schutzmassnahme wirkungslos.

Mit der folgenden HTTP-GET-Anfrage (ursprünglich eine HTTP-POST-Anfrage) wird die E-Mail-Adresse des eingeloggten Benutzers auf den im Query-Parameter *email* angegebenen Wert geändert:

```
GET /specialist-
edit.html?lastName=●●●●●●●●●●&firstName=●●●●●●●●●●&mobile=&email=controlledby
@attacker.com&ean=●●●●●●●●●●&submitted=true HTTP/1.1
Host: www.meineimpfungen.ch
Connection: close
sec-ch-ua: ●●●●●●●●●
sec-ch-ua-mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: ●●●●●●●●●
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicatio
n/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://attacker.com
Accept-Encoding: gzip, deflate
Accept-Language: de-DE,de;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: ●●●●●●●●●
```

Auszug 8 – Die von einer anderen Site kommende HTTP-GET-Anfrage zum Ändern der Fachpersonen-E-Mail (CSRF).

Anschliessend kann der Angreifer einen Passwort-Reset durchführen und den Benutzer-Account übernehmen.

Für eine erfolgreiche Account-Übernahme einer Fachperson ist die Kenntnis deren EAN bzw. GLN notwendig. Diese kann der öffentlichen, lizenzfreien *Partnerrefdatabase* der *Stiftung Refdata* unter *https://refdata.ch* entnommen werden.

Empfehlung

Unsichere HTTP-Anfragen bzw. solche, welche auf Seiten der Webanwendung möglicherweise ungewünschte Aktionen auslösen können (hier auch HTTP-GET-Anfragen), sollten bei Cookie-basierter Authentisierung stets ein durch einen Angreifer nicht erratbares Anti-CSRF-Token tragen[7].

Das Token sollte im HTTP-Anfrage-Header oder im HTTP-Message-Body positioniert sein und von der Webanwendung unbedingt auch verifiziert werden, bevor eine Aktion im Namen des authentifizierten Benutzers veranlasst wird. Das Token muss unabhängig für jeden Benutzer generiert werden und eine Entropie von zumindest 128 Bit besitzen. Zudem darf das Token nicht über Cross-Origin-Anfragen einsehbar sein, also beispielsweise nicht per Cross-Origin-Ressource-Sharing- (CORS) oder JSONP-Anfrage preisgegeben werden.

Viele CSRF-Verteidigungsmechanismen, wie das beschriebene Anti-CSRF-Token, können durch Ausnutzen von Cross-Site-Scripting-Schwachstellen (XSS) umgangen werden. Daher sollten insbesondere Aktionen mit hohem Schadpotential - wie das Löschen von Benutzerkonten - zusätzlich durch sog. Challenge-Response-Verfahren abgesichert werden.

[7] https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html

Hierrunter versteht man beispielsweise den Einsatz von Captchas, eine Re-Authentisierung oder den Einsatz von Einmalpasswörtern.

CSRF-Verteidigungsmassnahmen, welche auf den HTTP-Origin-Header setzen, sind allein nicht ausreichend. Einige Browser inkludieren diesen HTTP-Header noch nicht, zudem wird er nicht mit jeder HTTP-Anfrage gesendet.

Die Verwendung des "SameSite"-Cookie-Attributes ist als zusätzliche Schutzmassnahme empfohlen, schützt aber nicht alle Cross-Origin-Anfragen, beispielsweise im Fall eines Subdomain-Takeovers.

Alternativ stellt der Einsatz eines nicht auf Cookies basierenden Authentifizierungsverfahrens eine effektive Möglichkeit dar, CSRF-Angriffe von vornherein zu unterbinden.