Ergebnisreport Untersuchung «Nationales Organspenderegister»

durchgeführt von

ZFT.COMPANY GmbH

Autoren

Dr. André Zilch,
Sven Fassbender,
Martin Tschirsich

Version: 1.1
Datum: 18.01.2022

1 Inhaltsverzeichnis

2 ZUSAMMENFASSUNG 1

3 ÜBERSICHT DER BEFUNDE 2

4 BEFUNDE 3

4.1 Registrierung und Identitätsfeststellung auf ungenügendem Vertrauensniveau 3

4.2 Abgabe des Entscheids 5

4.3 Ungenügende Authentisierungsmechanismen 7

4.4 Auslesen von Dateien auf dem Server 8

4.5 Zugriff auf Lebertransplantationsdaten 10

2 Management Summary

Das aus dem Internet zugängliche *nationale Organspenderegister* dient der Erfassung von persönlichen Entscheiden zur Organspende.

Damit in der Schweiz Organe sowie Gewebe zur Spende oder zu Forschungszwecken entnommen werden dürfen, muss ein positiver Entscheid (Opt-In) des Betroffenen vorliegen.

Neben der Patientenverfügung oder dem physischen Organspendeausweis[1] stellt das Organspenderegister eine digitale Möglichkeit dar, einen solchen Entscheid zu dokumentieren.

Im Rahmen eines ehrenamtlichen Engagements wurden dabei jedoch kritische Sicherheitsmängel im Organspenderegister identifiziert.

Als Betreiberin und somit Verantwortliche des Registers ist die *Schweizerische Nationale Stiftung für Organspende und Transplantation* angegeben.

Der Webseite[2] wurden die folgenden Hinweise zum Datenschutz entnommen:

***Swisstransplant schützt die Vertraulichkeit und Sicherheit Ihrer personenbezogenen Daten**, die wir im Rahmen unserer Geschäftstätigkeit erheben und weiterbearbeiten. Wir bearbeiten persönlich Daten gemäss dem Schweizer Datenschutzgesetz (DSG) und, soweit anwendbar, der Datenschutzgrundverordnung der EU (DSGVO).*
...
*Wir bedienen uns im Übrigen **geeigneter technischer und organisatorischer Sicherheitsmassnahmen**, um Ihre Daten gegen zufällige oder vorsätzliche Manipulationen, teilweisen oder vollständigen Verlust, Zerstörung oder gegen den unbefugten Zugriff Dritter zu schützen. Unsere **Sicherheitsmassnahmen werden entsprechend der technologischen Entwicklung fortlaufend verbessert**.*

Bereits eine kursorische Untersuchung des Registers hat jedoch kritische Sicherheitsmängel aufgedeckt. In diesem Report wird nur auf Mängel mit hohem Risiko eingegangen, darunter insbesondere

- der mangelhafte Registrierungs- und Einwilligungsprozess,
- der ungenügende Authentisierungsmechanismus sowie
- eine unzureichende Prüfung der Eingabeparameter.

Auswirkung der identifizierten Mängel sind ein vollständiger Verlust der Vertraulichkeit, Authentizität und Integrität der im Organspenderegister erfassten Daten. Insbesondere ist nicht nachweisbar, wer welche Entscheide im Organspenderegister verfasst hat. Entscheide konnten mühelos und ohne Entdeckungsrisiko im Namen Dritter abgegeben werden.

Vor einem Weiterbetrieb des Organspenderegisters empfehlen wir die im Report nachfolgend gelisteten Massnahmen umzusetzen, die betroffenen Personen zu informieren sowie eine umfassende Sicherheitsüberprüfung durchzuführen.

Die identifizierten Mängel werden den Verantwortlichen in einem Coordinated-Disclosure-Verfahren mitgeteilt. Ziel ist, dass die identifizierten Mängel durch die Verantwortlichen behoben werden. Eine Veröffentlichung des Reportes erfolgt in Abstimmung mit den Verantwortlichen.

[1] https://www.deinadieu.ch/organspende/
[2] https://www.swisstransplant.org/de/datenschutz

3 Übersicht der Befunde

Nr.	Titel	Risiko
4.1	Registrierung und Identitätsfeststellung auf ungenügendem Vertrauensniveau	Hoch
4.2	Abgabe des Entscheids	Hoch
4.3	Ungenügende Authentisierungsmechanismen	Hoch
4.4	Auslesen von Dateien auf dem Server	Hoch
4.5	Zugriff auf Lebertransplantationsdaten	Hoch

4 Befunde

Dieser Abschnitt beinhaltet die detaillierte Beschreibung der identifizierten Schwachstellen.

4.1 Registrierung und Identitätsfeststellung auf ungenügendem Vertrauensniveau

Klasse	Registrierung
Risiko	Hoch

Die Identitätsfeststellung während des Registrierungsprozess erfolgt auf einem ungenügenden Vertrauensniveau. Dadurch ist die Authentizität der abgegebenen Einwilligungen nicht gewährleistet.

Aus den *Bedingungen für Einträge in das nationale Organspenderegister*[3] wurde der folgende Abschnitt entnommen. Bereits dieser dokumentiert den mangelhaften Prozess:

> ***«Online-Registereintrag:** Die eintragungswillige Person gibt die für den Eintrag in das Register erforderlichen Informationen in der Register-Applikation ein. Zur Identitätsfeststellung ist ein Foto der eintragungswilligen Person direkt in der Register-Applikation aufzunehmen oder ein Foto/Scan eines gültigen Ausweispapieres (ID/Pass) hochzuladen. Nach Abschluss des Prozesses ist das Datenblatt zu unterzeichnen. Je nach Eintragungsvariante wird das Datenblatt direkt auf dem Bildschirm oder erst nach dessen Ausdruck unterzeichnet. Qualifizierte elektronische Signaturen werden nur anerkannt, sofern ebenfalls die eigenhändige Unterschrift der eintragungswilligen Person erkennbar ist. Das unterzeichnete Datenblatt ist zur Überprüfung und Aktivierung des Eintrags Swisstransplant zuzustellen. Aufgrund der verschiedenen Eintragungsvarianten stehen hierfür verschiedene Möglichkeiten (Scan, Post, automatische Übertragung bei Prozessabschluss) zur Verfügung.»*

Allein mittels «Foto der eintragungswilligen Person» oder eines «Foto/Scan eines gültigen Ausweispapiers» lässt sich keine rechtsgültige Identitätsfeststellung durchführen.

Aufgrund der Manipulationsmöglichkeiten bei der Bereitstellung eines Fotos einer Person oder eines Scans eines Ausweisdokuments ist zu keinem Zeitpunkt der Registrierung gewährleistet, dass die Einwilligung auch durch die betroffene Person durchgeführt wird.

Es wird keine e-Signatur im Sinne des Gesetzes erzeugt – weder beim «unterzeichnen auf einem Bildschirm» noch bei der Übermittlung mittels E-Mail eines gescannten und unterzeichneten Entscheides. Lediglich im Falle, dass das Originalformular mit originaler Unterschrift per klassischer Post übermittelt wird und dieses originale Dokument dauerhaft aufbewahrt würde, liesse sich bei Zweifeln an der Einwilligung auf das Original zurückgreifen und ggf. gutachterlich prüfen.[4]

Die von *Swisstransplant* implementierten Verfahren unterscheiden sich grundsätzlich von Verfahren, die mittels "elektronische Signaturen" im Sinne Art. 14 Abs. 2bis des Obligationenrechtes (OR, SR 220) erzeugt werden.

Den durch *Swisstransplant* eingesetzten Verfahren mangelt es an einer

- entsprechend dem Schutzbedarf durchgeführten sicheren und zweifelsfreien Identifizierung des Unterzeichnenden sowie einer
- gültigen elektronischen Willenserklärung im Falle einer Unterzeichnung auf dem Bildschirm. Es liegt keine qualifizierte elektronische Signatur gemäss Artikel 14 Absatz 2bis Obligationsrecht (OR, SR 220) vor.

[3] Swisstransplant; Bedingungen für Einträge in das Nationale Organspenderegister; Online: https://register.swisstransplant.org/static/documents/bedingungen.pdf

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

Empfehlung

Die Identität der eintragungswilligen Person muss entsprechend des geforderten Vertrauensniveaus rechtsgültig durch vom Benutzer unabhängige und zulässige Instanzen festgestellt werden.

4.2 Abgabe des Entscheids

Klasse	Abgabe von Willenserklärungen
Risiko	Hoch

Die Abgabe des Entscheids erfolgt auf einem unzureichenden Vertrauensniveau. Die Authentizität der Unterschrift (Willenserklärung) kann hierbei nicht rechtsicher nachgewiesen werden.

Je nachdem, ob die eintragungswillige Person ein Mobilgerät verwendet, wird der Entscheid direkt auf dem Bildschirm oder erst nach dessen Ausdruck unterzeichnet.

Im zweiten Fall, bei Unterzeichnung auf dem Ausdruck, muss dieser anschliessend noch an *Swisstransplant* übermittelt werden. Hierfür stehen zwei Möglichkeiten[5] zur Verfügung:

- Scan des ausgedruckten und unterzeichneten Entscheids und Upload in der Webanwendung
- Versand des ausgedruckten und unterzeichneten Entscheids per Post

Abbildung 1 - Zwei Möglichkeiten zur Übermittlung des ausgedruckten und unterzeichneten Entscheids

Eine Willenserklärung auf hohem Vertrauensniveau wird dabei nur abgegeben, sofern

- der Entscheid ausgedruckt, händisch unterschrieben und als Original per Post an *Swisstransplant* übermittelt wird oder
- der Entscheid qualifiziert elektronisch signiert und digital an *Swisstransplant* übermittelt wird.

Im Falle der Übermittlung des Entscheids per Post liegt zwar eine den Anforderungen entsprechende Willenserklärungen vor, jedoch fehlt es an einer Identitätsprüfung auf gleichem Vertrauensniveau gemäss Befund 4.1, so dass nicht sichergestellt ist, dass der Entscheid auch tatsächlich von der im Entscheid benannten Person unterzeichnet wurde.

Auch wenn in der Schweiz prinzipiell mit Kopien gearbeitet werden kann, so muss bei Zweifeln doch das Original vorgelegt werden können. Dies ist aber bei Verfahren, die entweder vollständig digital, aber ohne qualifizierte elektronische Signatur (Unterschrift auf dem Bildschirm) oder mit Scans von

[5] Swisstransplant; Bedingungen für Einträge in das Nationale Organspenderegister; Online: https://register.swisstransplant.org/static/documents/bedingungen.pdf

ausgedruckten und unterschriebenen Entscheiden, die per E-Mail versandt werden, schlichtweg unmöglich.[6]

Im Zweifel muss *Swisstransplant* nachweisen können, dass eine Willenserklärung auf hohem Vertrauensniveau durch die im Profil beschriebene Person vorliegt.

Im Rahmen der durchgeführten Analyse wurde exemplarisch ein Entscheid mittels Unterschrift auf einem Bildschirm eines Mobilgerätes im Namen einer dritten Person erzeugt und an Swisstransplant übermittelt. Das auf diese Weise übermittelte Datenblatt wurde von Swisstransplant als «wahr» klassifiziert und das entsprechende Profil aktiviert.

In einem weiteren Versuch wurde ein ausgedruckter Entscheid durch eine andere als im Profil beschriebene Person unterzeichnet, eingescannt und an *Swisstransplant* übermittelt. Auch in diesem Fall erfolgte eine kurzfristige Freigabe durch *Swisstransplant*.

Auf diese Weise konnten beliebige Dritte zu Organspendern erklärt werden, ohne dass diese davon Kenntnis nehmen konnten oder zustimmen mussten. Da durch die beschriebenen Verfahren nicht sichergestellt werden kann, dass der Entscheid durch die eintragungswillige Person unterzeichnet wurde, müssen alle bisher vorhandenen Entscheide als kompromittiert angesehen werden.

Die in den Abläufen von *Swisstransplant* geforderten Nachweise (Bild der Person, Foto eines Ausweises, gescannter Entscheid mit Unterschrift) sowie die Abläufe selbst zur Dokumentation der Willensbekundung können nicht sicherzustellen, dass die Willensbekundung ausschliesslich durch die im Profil beschriebene Person erfolgt.

Empfehlung

Die Entscheide sind als nicht authentisch anzusehen und müssen dahingehend verifiziert werden, inwieweit sie tatsächlich von der jeweiligen Person unterzeichnet wurden. Die Abläufe, Nachweise und die Art der Dokumentation der Einwilligungen sind gemäss Stand der Technik zu überprüfen und anzupassen.

[6] BGer 9C_634/2014 vom 31.08.2015

4.3 Ungenügende Authentisierungsmechanismen

Klasse	Authentisierung
Risiko	Hoch

Das Organspenderegister authentifiziert Nutzer zusätzlich zum Passwort anhand eines Codes, welcher per E-Mail oder SMS zugestellt wird. Die Mindestanforderungen an eine sichere Zwei-Faktor-Authentifizierung werden dabei nicht erfüllt.

Eine Authentisierung mittels Passworts allein erreicht lediglich ein niedriges Vertrauensniveau, welches hinsichtlich der Abgabe der Willenserklärung der eintragungswilligen Person nicht ausreichend ist.

Eine dem Stand der Technik entsprechende Authentisierung auf hohem Vertrauensniveau bedingt eine sichere Zwei-Faktor-Authentifizierung (2FA). 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 der eintragungswilligen Person.

Die im Falle des nationalen Organspenderegisters eingesetzten Authentisierungsmechanismen entsprechen nicht den oben dargelegten Anforderungen an eine 2FA. Ein per SMS oder E-Mail verschickter Code erfüllt nicht die Anforderungen an einen Besitzfaktor. Allein der Zugriff auf eine E-Mail ist ausreichend, um ohne weiteren Faktor eine erfolgreiche Authentisierung durchzuführen.

Empfehlung

Der Authentisierungsmechanismen ist auf eine datenschutzkonforme 2FA entsprechend dem Schutzbedarf der hinterlegten Entscheide umzustellen.

4.4 Auslesen von Dateien auf dem Server

Klasse	Local File Inclusion (LFI)
Risiko	Hoch

Fehlende Validierung von Pfadangaben erlaubt einem nicht authentisierten Angreifer das Auslesen von beliebigen Dateien des Anwendungsservers aus dem öffentlichen Internet. Da die Anwendung mit Root-Rechten ausgestattet ist, kann auf alle Dateien zugegriffen werden.

Der Zugriff auf beliebige Dateien des Anwendungsservers des Organspenderegisters ist möglich, da eine sogenannte Local-File-Inclusion (LFI)-Schwachstelle vorliegt. Diese Schwachstellen treten häufig auf, wenn Benutzereingaben serverseitig ohne Bereinigung weiterverarbeitet werden. Werden diese Eingaben als Bestandteil eines Dateipfades für den Zugriff auf lokale Dateien verwendet, kann ein Angreifer durch Angabe sog. Dot-Segments wie beispielsweise *../../../../../* auf Dateien ausserhalb des vorgesehenen Verzeichnisses zugreifen.

Im Test wurde durch einen nicht authentisierten Nutzer folgende HTTP-GET-Anfrage an den Anwendungsserver gesendet, wobei der Pfad der abzurufenden Datei über den HTTP-GET-Parameter *fileName* gegeben ist:

```
GET
/javax.faces.resource/dynamiccontent.properties.xhtml?ln=primefaces&v=6.2.19&pfdri
d=[redigiert]&pfdrt=sc&fileName=../../../../../../etc/shadow&imagePath=image&regis
trationId=[redigiert]&pfdrid_c=false&uid=[redigiert] HTTP/1.1
Host: register.swisstransplant.org
Referer:
https://register.swisstransplant.org/pages/public/registrationWizard.xhtml?lang=de
Connection: close
```

Die entsprechende HTTP-Antwort enthält den Inhalt der abgerufenen Datei */etc/shadow*:

```
HTTP/1.1 200 200
Date: [redigiert]
Server: Apache
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: Mon, 8 Aug 1980 10:00:00 GMT
Vary: Accept-Encoding
Connection: close
Content-Type: application/xhtml+xml
Content-Length: 1193

root:$6$[redigiert]:17737:0:99999:7:::
[snip]
bgsansible:$6$[redigiert]:17737:0:99999:7:::
bgsadmin:$6$[redigiert]:17737:0:99999:7:::
[snip]
sweng:$6$[redigiert]:17737:0:99999:7:::
```

Wie dieses Beispiel zeigt, ist die Schwachstelle als nicht authentisierter Benutzer ausnutzbar und wird mit erhöhten Privilegien (root) ausgeführt. Dies bedeutet auch, dass unter Zugriff auf das virtuelle Prozessdateisystem *procfs* sensible Dateien des Anwendungsservers wie Logdateien mit personenbezogenen Daten der eintragungswilligen Personen ohne Kenntnis exakter Dateipfade abgerufen werden können.

Wie oben geschildert kann ein Angreifer mit Zugriff auf diese aus dem öffentlichen Internet zugängliche Schnittstelle – durch Erraten der Dateien auf dem Dateisystem – auf sensible Daten zugreifen.

Empfehlung

Es sollte vermieden werden, Benutzereingaben ohne vorherige Prüfung zum Abruf von Dateien oder Verzeichnissen zuzulassen. Eine Prüfung der Benutzereingaben sollte immer gegen eine White-List von vertrauenswürdigen Eingaben erfolgen[7].

Ausserdem sollte die Anwendung mit einem möglichst niedrig privilegierten Benutzer ausgeführt werden (Principle-of-Least-Privilege).

[7] https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/07-Input_Validation_Testing/11.1-Testing_for_Local_File_Inclusion

4.5 Zugriff auf Lebertransplantationsdaten

Klasse	Autorisierung
Risiko	Hoch

Ein Fehler bei der Prüfung der Autorisierung in der Web-Anwendung erlaubt einen Zugriff auf Lebertransplantationsdaten für nicht autorisierte Benutzer.

Neben dem nationalen Organspenderegister betreibt die verantwortliche Stiftung weitere Anwendungen, darunter das «Lifeport Kidney Perfusion Machine Protocol and Donor Evaluation Register».

Vor Zugriff auf diese Anwendung muss ein Registrierungsprozess durchlaufen werden. Dieser beinhaltet unter anderem eine Freischaltung des Accounts durch die Betreiberin. Jedoch ist bereits ein Zugriff auf Daten möglich, bevor die Freischaltung erfolgt ist.

Hierzu wird zunächst eine Registration über das entsprechende Web-Formular gestartet:

- https://app.swisstransplant.org/#!/signup

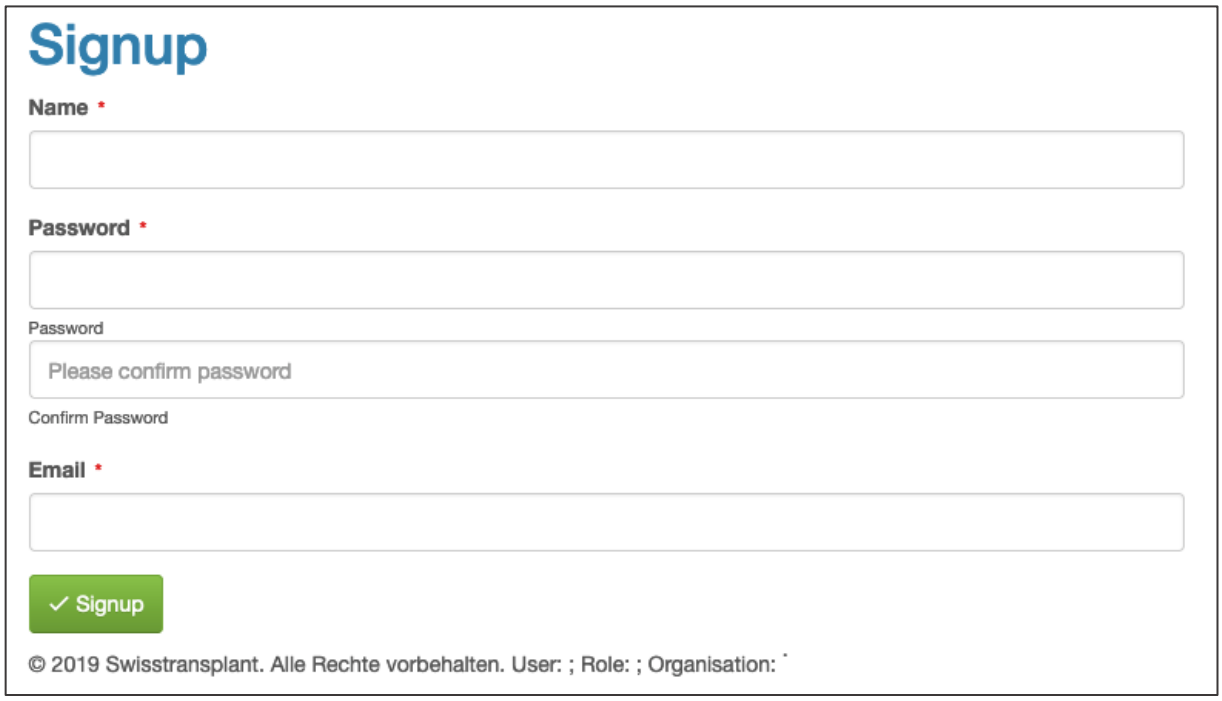

Abbildung 2 - Signup-Maske der Web-Anwendung

Nachdem der Antrag durch einen Klick auf «Signup» versendet wurde, kann auf Inhalte zugegriffen werden. Hierzu kann beispielsweise die folgende HTTP-POST-Anfrage an das System gesendet werden:

```
POST /webapi/v1/app/g/[...redigiert...] HTTP/1.1
Host: app.swisstransplant.org
Cookie: [...redigiert...]
Content-Length: 238
X-Xsrf-Token: [...redigiert...] Sec-Ch-Ua-Mobile: ?0
Content-Type: application/json;charset=UTF-8
Accept: application/json, text/plain, */*
X-Tb-Token: [...redigiert...]
Sec-Ch-Ua-Platform: "macOS"
Origin: https://app.swisstransplant.org
Sec-Fetch-Site: same-origin
```

```
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://app.swisstransplant.org/
Accept-Encoding: gzip, deflate
Accept-Language: de-DE,de;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close

{"filters":{"k":""},"page":1,"fIndex":-1,"rId":""}
```

Die Server-Antwort enthält beispielsweise Einträge, welche von registrierten Fachpersonen erstellt wurden:

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: Content-Type, X-Auth-Token, Origin, X-Tadabase-App-
id, X-Tadabase-App-Key, X-Tadabase-App-Secret
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Origin: *
Cache-Control: no-cache, private, max-age=172800
Content-Type: application/json
Date: [...redigiert...]
Expires: [...redigiert...]
Server: Fly.io (dcf56d0)
Set-Cookie: [...redigiert...]
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Powered-By: Tadabase.io
X-Protected-By: Sqreen
X-Tb-Server: TB-S-4
X-Xss-Protection: 1;mode=block
Content-Length: 4625
Connection: close

{"sortby":[{"sort":"id","by":"desc"}],"items":[{"id":"[...redigiert...]","field_60
9":{"[...redigiert...]":""},"field_610":"Aufgrund des geringen Anstiegs der
Transaminasen w\u00fcrden wir den Patienten als Spender einschliessen - allerdings
Entnahme etwas verz\u00f6gert - idealerweise 20.5. und weiterhin Verlauf der
Transaminasen, CK, CK.MB und Kreta idealerweise 8-stdl.
Danke.","field_611":"","field_612":"","field_613":"","field_614":"","field_621":[]
},
[…]
```

Die Kommentare der Fachpersonen enthalten – gemäss oberflächlicher Betrachtung – keine Angaben, welche ohne weitere Quellen einem Patienten zugeordnet werden können. Dennoch kann nicht ausgeschlossen werden, dass ein Angreifer über weitere Informationen verfügt, welche zur Bestimmung der Personalie führen.

Darüber hinaus scheint auch eine Manipulation der Datensätze möglich zu sein. Von einer Demonstration (Proof-of-Concept) wurde in diesem Fall abgesehen.

Empfehlung

Es wird empfohlen ein Benutzer- und Rollenkonzept mit Prüfung der Autorisierung zu implementieren. Hierbei ist darauf zu achten, dass ein Fachpersonen-Account erst berechtigt wird, wenn die Authentizität der Fachperson auf geeignetem Weg sichergestellt wurde.