Ablauf der Adressierung der DiGA-Schwachstelle bzgl. Datensicherheit

[redacted]

04.04.2022: Meldung der Sicherheitslücke durch Zerforschung an CERT-Bund, den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, das Bundesinstitut für Arzneimittel und Medizinprodukte, die [redacted] und der [redacted] [redacted] (Hersteller von [redacted])

05.04.2022: E-Mail von [redacted] an alle, dass die Softwareentwicklenden die Sicherheitslücken analysiert und diese bereits geschlossen haben

05.04.2022: Aufforderung zur Stellungnahme durch das BfArM mit Frist 08.04.2022

07.04.2022: Ausführliche Stellungnahme zur Sicherheitslücke, deren Behebung sowie der daraus abgeleiteten Maßnahmen von [redacted]

29.04.2022: Vom BfArM initiiertes Telefonat mit [redacted] (Zerforschung) über die gefundenen Sicherheitslücken bei den DiGA [redacted] und [redacted] [redacted]

[ZER-2022-015] Sicherheitslücken in Novego DiG
A
zerforschung <hallo@zerforschung.org>
An: CERT-Bund <certbund@bsi.bund.de>
mailbox@datenschutz.hamburg.de
[redacted]
Datum: 04.04.2022 12:11:38

Sehr geehrte Mitarbeiter*innen des CERT-Bund, des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, des Bundesinstitut für Arzneimittel und Medizinprodukte, der [redacted] und der [redacted],

Wir wenden uns heute mit einem Responsible-Dislcosure-Bericht zum Webportal "[redacted]" mit der PZN [redacted]" von der [redacted] an S e.

Im Rahmen einer unabhängigen zivilgesellschaftlichen Sicherheitsüberprüfung haben wir eine schwerwiegende Sicherheitslücke im Portal "[redacted]" gefunden, die Zugriff auf personenbezogenen Daten wie z.B. E-Mail-Adresse, Nutzernamen, Geschlecht und Diagnose einer fünfstelligen Anzahl von Nutzer*innen erlaubt. Hierbei handelt es sich um Gesundheitsdaten - also besonders schützenswerte Daten nach Art. 9 DSGVO. Diese ist im PDF im Anhang ausführlicher beschreiben.

Wir bitten das Unternehmen uns den Empfang dieser Nachricht unmittelbar zu bestätigen und uns einen Zeitplan zum Schließen der Lücke mitzuteilen.

Die persönliche Ansprechpartnerin für diesen Fall bei uns im Haus ist [redacted] von Zerforschung, die unter der E-Mail-Adresse hallo@zerforschung.org sowie telefonisch unter [redacted] zur Verfügung steht.

Viele Grüße,
zerforschung

ZER REVERSE ENGINEERING ZENTRUM

Datenabfluss bei [redacted]

ID: [redacted]

Score: [redacted]

Initial Version: 2022-04-04
Last Update: 2022-04-04

1 Beschreibung

Das Unternehmen

[redacted]

betreibt das Therapieportal "[redacted]". Dieses ist unter dem Namen "[redacted]" mit der PZN "[redacted]" seit dem 10.10.2021 für die Behandlung bei folgenden Erkrankungen vorläufig zugelassen:

```
F32.0 Leichte depressive Episode

F32.1 Mittelgradige depressive Episode

F33.0 Rezidivierende depressive Störung, gegenwärtig leichte Episode

F33.1 Rezidivierende depressive Störung, gegenwärtig mittelgradige
Episode

F34.1 Dysthymia
```

2 Auswirkungen

Die Sicherheitslücke ermöglicht das Abrufen von personenbezogenen Daten wie z.B. E-Mail-Adresse, Nutzernamen, Geschlecht und Diagnose einer fünfstelligen Anzahl von Nutzer*innen. Hierbei handelt es sich um Gesundheitsdaten – also besonders schützenswerte Daten nach Art. 9 DSGVO.

3 Schritte zum Nachvollziehen der Lücke (Steps to Reproduce)

1. Anlegen eines Accountes und Login auf [redacted].
2. Abrufen des URL-Endpunktes

[redacted]
(z.B. [redacted]

3. Die Antwort des Webservers beinhaltet eine URL im Format

[1] [redacted]

4. Nach mindestens 2 Sekunden die URL aus Schritt 3 aufrufen. Eine ZIP-Datei wird heruntergeladen.
5. Diese ZIP-Datei enthält eine Reihe von XML-Dateien mit den personenbezogenen Daten der Patient*innen.

4 Kontaktinformationen

Für technische Rückfragen stehen wir unter der E-Mail-Adresse hallo@zerforschung.org zur Verfügung. Verschlüsselte Kommunikation ist mittels S/MIME mit dem auf unserer Kontakt-Seite verlinkten Zertifikat möglich.

Ihre persönliche Ansprechpartnerin ist [redacted]. Sie erreichen sie jederzeit unter [redacted].

5 Verweise

Auf der Website konnte kein Security-Kontakt gefunden werden. Wir empfehlen, diesen mittels des security.txt-Standards bereitzustellen.

6 Versionshistorie

Version	Datum	Beschreibung
1	2022-04-04	Initiale Version

Bundesinstitut
für Arzneimittel
und Medizinprodukte

BfArM, Kurt-Georg-Kiesinger-Allee 3, D-53175 Bonn

[redacted]

ABTEILUNG Medizinprodukte
BEARBEITET VON Dr. Armin Grünewald
TEL +49 (0)228 99 307[redacted]
E-MAIL [redacted].de

HAUSANSCHRIFT Kurt-Georg-Kiesinger-Allee 3
53175 Bonn
TEL +49 (0)228 99 307-0
FAX +49 (0)228 99 307-5207
E-MAIL poststelle@bfarm.de
INTERNET www.bfarm.de

Per E-Mail an: [redacted]

Bonn, 05.04.2022
GESCHZ [redacted]

Ihre digitale Gesundheitsanwendung im Verzeichnis nach § 139e Fünftes Buch Sozialgesetzbuch (SGB V)

Name der DiGA: [redacted]
Hersteller: [redacted]
DIGA-ID: [redacted]
Versionsnummer der digitalen Gesundheitsanwendung: [redacted]
Softwareversion: [redacted]

Aufforderung zur Stellungnahme bzgl. des Schreibens des ZER vom 04.04.2022

Sehr geehrter Herr [redacted],

das Reverse Engineering Zentrum (ZER) hat uns im Rahmen einer Sicherheitsuntersuchung darauf aufmerksam gemacht, dass über eine Sicherheitslücke in Ihrem Therapieportal „[redacted]“ personenbezogene Daten abgerufen werden können. Gemäß Anforderung 4 der Anlage 1 der Digitale Gesundheitsanwendungen-Verordnung (Datensicherheit) muss zu jeder Zeit sichergestellt sein, dass keine ungewollte Datenkommunikation aus der DiGA erfolgen kann.

In Ihrer Antwort-E-Mail an das ZER vom 04.04.2022 geben Sie an, dass die Sicherheitslücke bereits geschlossen wurde. Bitte legen Sie ausführlich dar, was Gegenstand und Hintergrund der Sicherheitslücke war, wie die Behebung dieses Mangels erfolgt ist, ob und warum Sie dies als hinreichend und zuverlässig erachten und welche weiteren Maßnahme Sie ggf. noch einleiten werden, um ähnliche Vorfälle zu verhindern.

Wir bitten Sie um Stellungnahme bis Freitag, den 08.04.2022 um 12 Uhr an diga@bfarm.de.

Mit freundlichen Grüßen
Im Auftrag

Dr. Armin Grünewald

Dieses Schreiben enthält in Übereinstimmung mit § 33 Absatz 3 Satz 1 SGB X nur eine Namenswiedergabe und keine Unterschrift.

[redacted]

Bericht zum Datenschutzvorfall [redacted] vom 04.04.2022

Internes Aktenzeichen: 20220404 Datenabfluss bei [redacted]

Kategorie des Vorfalls: Softwarefehler (Bug) / Datenabfluss

Zeitpunkt/Zeitraum, des Verstoßes: 06.08.2021 – 04.04.2022

Datum und Uhrzeit der Feststellung des Verstoßes: 04.04.2022 12:12 Uhr

Sachverhalt:

Am 04.04.2022 erhielten wir von der Emailadresse hallo@zerforschung.org durch das zerforschung Team eine Mitteilung an [redacted], dass durch die Ausnutzung einer Sicherheitslücke im [redacted] Webportal ein unberechtigter Zugriff auf personenbezogene Daten möglich sei. Im Rahmen des DiGA Zulassungsprozesses und der damit einhergehenden Anforderung der Interoperabilität von Daten, wurde im August 2021 ein Feature releast, welches das einfache Runterladen der personenbezogenen Daten für den einzelnen Nutzer erlauben muss. Im Rahmen des Downloads der Daten (über einen Button) wird eine URL erzeugt, die eine individuelle Nutzer ID für jeden Nutzer enthält. Ist ein Nutzer im Webportal eingeloggt, so war es dem Nutzer theoretisch durch die Anpassung/Veränderung der Nutzer ID (in der vorher generierten URL) zwischenzeitlich möglich, auch fremde Nutzerdaten herunterzuladen. Ein theoretisches Ausnutzen dieser Sicherheitslücke war ausschließlich registrierten Nutzern mit einem entsprechenden IT-Verständnis und Know How möglich. Dem normalen Nutzer blieb diese Schwachstelle verborgen, da es keinerlei Möglichkeit gibt auf den Seitenquelltext zuzugreifen und auch die Download URL nicht explizit angezeigt wird. Vor dem dankeswerten Hinweis des zerforschung Teams gab es keinerlei Hinweise bzw. Rückmeldungen von Patienten oder anderweitigen Organisationen, welches auf ein Ausnutzen dieser Schwachstelle hinweist.

Aus unserer Sicht ist zusammenfassend folgendes Vorgehen notwendig, um die Sicherheitslücke ausfindig zu machen:

1. [redacted]-Account anlegen
2. [redacted]-Account mit Verifizierung der E-Mail-Adresse bestätigen
3. Auf der [redacted] Website einloggen
4. Zum Bereich Datenexport navigieren
5. Versteckte URL hinter dem Button "Profil export" finden und extrahieren (nur mit speziellen IT Knowhow, nicht für normale Nutzer, möglich)
6. Auf den Button „Profil export“ klicken (Dadurch wird ein neuer Downloadlink im Hintergrund generiert und Button „Profil export“ wird durch den Button "Datei herunterladen" ersetzt)
7. Den im Punkt 6 generierten und versteckten Downloadlink extrahieren (nur mit speziellen IT Knowhow, nicht für normale Nutzer, möglich)
8. Analyse sowohl der "Profil export URL" als auch "Download URL" und Austausch der Nutzer ID in beiden URLs.
9. Wiederholung von Austausch der Nutzer ID für jeden einzelnen Datensatz (Nutzer)
10. Aufruf von beiden manipulierten Links in entsprechender Reihenfolge

[redacted]

Art der betroffenen Daten:

Theoretisch wäre durch die Sicherheitslücke ein Zugriff auf personenbezogene Daten (inkl. Gesundheitsdaten nach Art 9 DSGVO) möglich gewesen (Email-Adresse, Name, Geschlecht, Anschrift, Zahlungsdaten). Da es sich bei den meisten Eingaben der Nutzer jedoch um keine Pflichtfelder handelt, ist der Datenumfang für jeden einzelnen Nutzer sehr individuell und in den allermeisten Fällen sehr gering. Im speziellen Anwendungsfall vom zerforschung Team, handelte es sich ausschließlich um die Emailadresse des Nutzers sowie seinen frei gewählten Benutzernamen. Ein einfacher Massenexport aller Nutzerdaten war zu keiner Zeit möglich, vielmehr muss die Abfrage der URL für jede einzelne Nutzer ID wiederholt werden. Über das datenschutzkonforme Analyse- Tool Matomo konnte nur der Fall des zerforschungs Team rekonstruiert werden, sodass von keinen weiteren Fällen auszugehen ist.

Ergriffene technische und organisatorische Maßnahmen:

Unmittelbar nach der Mitteilung von zerforschung wurde die Information über die Sicherheitslücke vom Projektmanagement an die Leitung der IT-Entwicklung übermittelt. Daraufhin wurde die Sicherheitslücke von unseren Softwareentwicklern geprüft und noch am selben Tag (innerhalb von 3 Stunden) geschlossen. Um die Sicherheitslücke zu schließen, wurde in den Code eine Überprüfung eingebaut, ob die gerade angemeldete Nutzer ID der an die URL übergebenen ID entspricht. Sind diese beiden Nutzer IDs nicht identisch, ist ein Download der personenbezogenen Daten nicht möglich und es erfolgt eine Weiterleitung auf eine „404 Fehlerseite“. Diese Überprüfung der beiden IDs entspricht dem momentanen und neusten Stand der Technik und wird allgemein als sicher eingestuft. Ein Download von fremden Daten durch die Veränderung der Nutzer ID in der URL ist somit technisch nicht mehr möglich. Die Interoperabilität wird bei einem rechtmäßigen Zugriff auf die Daten nicht eingeschränkt.

Ein IP Tracking auf der Website erfolgt nicht und es werden keine Web-Logfiles erstellt. Über das datenschutzkonforme Analyse-Tool Matomo konnte kein weiterer unberechtigter Datenzugriff und Datenabfluss festgestellt werden, welches auf einen Einzellfall hindeutet.

Über die rein technischen Maßnahmen, um den Gesamtschaden abschätzen zu können und die Sicherheitslücke unmittelbar zu schließen, wurden weitere organisatorische Maßnahmen eingeleitet bzw. angestoßen. Im Zuge der Sicherheitslücke wurde das Team der Softwareentwickler sowie das Projektmanagement erneut für das Thema Datenschutz und Informationssicherheit sensibilisiert und weitere Schulungen und Workshops zur Prozessverbesserung sind in Vorbereitung. Überdies wurde sich entschlossen zeitnah einen erneuten Pentest durchzuführen. Schlussendlich wurde mit unserem externen Datenschutzbeauftragten in den Austausch gegangen

Anzahl der Betroffenen: 1

[redacted], 07.04.2022

[redacted]

[redacted]