Sicherheitslücke in AOK Bonus-App entdeckt
Bericht: Romy Heinrich, Simon Köppl, Pauline Vestring

In diesem Bootcamp schwitze ich nicht ganz freiwillig. Ich quäle mich hier für die Bonus-App meiner Krankenkasse. Wenn ich am Tag eine von drei Fitness-Aktivitäten nachweisen kann, wird das belohnt. Dafür muss ich meinen Puls zum Beispiel für eine halbe Stunde auf mindestens 120 treiben.

Romy Heinrich, MDR-Reporterin
„Gemessen wird das mit meinem Fitnesstracker. Und meine Krankenkasse schreibt mir dann einen Bonus gut. Ich bin bei der AOK versichert, da könnte ich im Jahr bis zu 180 Euro verdienen."

Mit mir nutzen die Bonus-App in Sachsen und Thüringen 65.000 AOK-Versicherte. Die haben letztes Jahr mehr als neun Millionen Euro Boni von der Kasse ausgezahlt bekommen. Und so werden die Gesundheitsdaten übertragen:

Mit einem Fitnessarmband werden Daten, wie zum Beispiel Puls oder Schritte aufgezeichnet. Damit die Daten auf das Smartphone übertragen werden, muss das Fitnessarmband mit einer Fitness-App gekoppelt werden. In dieser werden die Daten auch gespeichert. Auf die Fitness-App greift die Bonus-App der Kasse zu. Dabei wird geprüft, ob eine Fitnessaktivität erfolgreich absolviert wurde. Dann werden die Bonuspunkte zur Kasse übertragen.

Doch ist es eine gute Idee, Fitness-Apps mit meinen Gesundheitsdaten zu füttern? Wir fahren nach Berlin zur Datenschützerin Katharina Nocun. Sie hat dazu eine klare Meinung:

Katharina Nocun, **Netzaktivistin und ehemalige Politikerin der Piratenpartei**
„Das Problem ist, dass wir gar nicht abschätzen können, was in Zukunft aus unseren Daten herauslesbar ist. Ich würde grundsätzlich keine sensiblen Daten in eine Krankenkassen-App eingeben. Die Krankenkasse kann mir natürlich versprechen: Wir haben nur diese Daten, wir haben nur jene Daten aber im Endeffekt wenn man kein Technik-Experte ist, muss man vertrauen."

Ich frage den IT-Sicherheits-Experten Jan. Er möchte selbst so wenige Daten wie möglich von sich preisgeben, sodass er seinen Nachnamen nicht veröffentlichen will. Zuerst schauen wir uns den Datenfluss der Fitness-App an. Vor zwei Jahren hat die Verbraucherzentrale bereits festgestellt, dass Fitness-Apps fast immer sensible Daten ins Ausland schicken.

Das hieße, meine Gesundheitsdaten würden von der Fitness-App ins Ausland gesendet, noch bevor sie zur Bonus-App gelangen. Das zeigt leider auch unser Test: Meine Daten landen auf einem Server an der Ostküste der USA. Meine Krankenkasse nimmt das also einfach in Kauf. Die AOK schreibt uns: „Es gibt leider keinen deutschen Schrittzähler, der an Google & Co. vorbeiführt." Doch was wollen amerikanische Unternehmen mit meinen Gesundheitsdaten?

Katharina Nocun, Netzaktivistin und ehemalige Politikerin der Piratenpartei
„Eine Möglichkeit ist, dass in den Geschäftsbedingungen ein Passus versteckt ist, dass diese Daten für Werbung genutzt werden können. Personalisierte Werbung ist ja ein Milliardengeschäft weltweit."

Außerdem sind Gesundheitsdaten auch für Versicherungen, Banken und Arbeitgeber interessant. In anderen Ländern ist der digitale Versicherte schon lange Alltag. In Israel werden seit 20 Jahren die Gesundheitsdaten aller Patienten umfassend digital gespeichert. Zum Beispiel Gewicht, Blutdruck oder Medikamente.

Auf diese Daten können neben Ärzten auch Forscher zugreifen. So lassen sich automatisiert Patienten nach bestimmten Merkmalen durchsuchen. Um zum Beispiel um Risikofaktoren für Schlaganfälle zu erkennen. Schon jetzt werden beschwerdefreie Patienten in Krankenhäuser bestellt, die ein erhöhtes Schlaganfall-Risiko haben. Ein denkbares Szenario auch für Deutschland, sagt Sebastian Schmidt-Kaehler. Er berät Krankenkassen bei Zukunftsprojekten zur Digitalisierung.

Sebastian Schmidt-Kaehler, Gesundheitswissenschaftler
„Und das ist gerade bei kritischen Ereignissen wie Schlaganfällen ein unglaubliches Potential auf der einen Seite Krankheiten zu verhindern, aber auf der anderen Seite für die Versicherungen Ausgaben herabzusetzen. Denn wenn sowas frühzeitig behandelt werden kann, ist das auf der Kostenseite was ganz anderes als wenn es zum schweren Schlaganfall kommt."

Also wenn sich Versicherte tracken lassen, sparen die Kassen richtig. In den USA geht man schon einen Schritt weiter: Dort bietet die Versicherung John Hancock bereits Tarife mit Tracking-Pflicht. Wer sich nicht überwachen lässt, für den wird es teuer. Dabei möchte der Versicherung sogar wissen, was die Kunden essen und tauscht dafür Daten aus. Auch in Deutschland wirbt eine Lebensversicherung damit, dass sie unter anderem den Kauf von Gemüse belohnt. Kunden können sogar bis zu 15 Prozent der jährlichen Versicherungsprämie sparen. Nächstes Jahr soll das Programm auf die Krankenversicherung übertragen werden.

In Deutschland dürfen die gesetzlichen Kassen für fitte Menschen keine Sonder-Rabatte gewähren. Sie werden per Bonus-App belohnt. Die AOK verspricht: Dazu werden keine Fitness- oder Vitaldaten übermittelt. Aber stimmt das wirklich?

Für unseren Test entschlüsselt Jan die Daten, die die App sendet und empfängt. Zur Kasse selbst werden wie versprochen nur meine 400 gesammelten Bonuspunkte übertragen. Die App scheint sicher. Doch dann entdecken wir eine Sicherheitslücke, die wir überhaupt nicht erwartet hätten: Jan kann problemlos mein AOK-Passwort auslesen.

Dieses Passwort ist auch der Zugang zur Online-Filiale. Wer jetzt noch meine SMS abfangen kann, der kann sehen, bei welchen Ärzten ich war - und was die abgerechnet haben. Und sogar, was mein Arbeitgeber in meine Rentenversicherung einzahlt.

Ich bin geschockt. Die AOK selbst will zur Sicherheitslücke vor der Kamera nicht sprechen, schriftlich heißt es: „Danke, dass Sie uns mit Ihrer Recherche auf eine bislang unentdeckte „Schwachstelle“ in unserer Bonus-App hingewiesen haben und uns damit die Chance eröffnen, diese zu verbessern.“

Die AOK-Verantwortlichen reagieren sofort, erwägen sogar ihre Bonus-App abzuschalten. Sie versuchen nach eigener Aussage tagelang den Test nachzustellen. Erst mit Hilfe unseres IT-Spezialisten finden sie die Sicherheitslücke - und schließen sie.

Das sächsische Sozialministerium ist die zuständige Aufsichtsbehörde, die die App auch genehmigt hat. Sie verspricht: *„Von aufsichtsrechtlicher Seite wird die Überarbeitung der AOK PLUS Bonus-App weiter verfolgt und begleitet.“*

Mir hat unser Test gezeigt, meine Kasse verarbeitet wirklich keine Gesundheitsdaten von mir.

Romy Heinrich, MDR-Reporterin
„Trotzdem hab ich ein ungutes Gefühl: Meine Daten landen in den USA und ich hab keine Ahnung, für was sie genau verwendet werden. Außerdem wurde mein Passwort gehackt. Auch wenn die AOK behaupte, dass sie das Problem inzwischen gelöst hat: Sichere Gesundheitsdaten stelle ich mir anders vor. Da verzichte ich lieber auf meinen Fitnesstracker und meinen Krankenkassen-Bonus.“

Das große Geschäft mit meinen Daten machen am Ende andere.