Sichere und vertrauenswürdige Apps oberstes Gebot

Selfpass: Mit Wearables gegen Depressionen

Depressionen gehören mit zu den am stärksten zunehmenden Begleiterscheinungen einer modernen Zivilisation. Im Projekt Selfpass sollen beim Kampf gegen Depressionen neue Methoden zum Einsatz kommen, darunter auch Wearables in Verbindung mit entsprechenden Smartphone-Apps. Die über Geräte wie Fitnessarmbänder gemessenen Vital- und Umweltparameter liefern Daten, die über eine intelligente Auswertung sehr zeitnah wertvolle Hinweise über den aktuellen Gemütszustand geben. Droht ein Stimmungsabfall, soll die App passgenaue Empfehlungen für sofort umsetzbare Verbesserungsmaßnahmen anbieten. Selfpass soll eine professionelle Therapie nicht ersetzen, möglicherweise begleiten, wenn der Arzt das für sinnvoll hält. In erster Linie geht es bei dem Projekt aber darum, die oft lange Zeit zwischen Erstdiagnose und Therapiebeginn überbrücken zu helfen. Für den Schutz der sensiblen persönlichen Daten steht Konformität mit der neuen DS-GVO an oberster Stelle.

Depressionen wurden lange unterschätzt. Inzwischen belegen zahlreiche Studien den Ernst der Lage. Eine Langzeiterhebung unter den 2,9 Millionen Mitgliedern der DAK-Versicherung von 1997 bis 2017 etwa kam zu dem Ergebnis, dass die Zahl psychischer Erkrankungen, die zu einer Arbeitsunfähigkeit führte, bei den Frauen um 284 Prozent zunahm[1]. Bei den Männern ist die Zunahme an Depressionen nur geringfügig niedriger. Auch im Vergleich aller Krankheiten, die in Deutschland im Jahr 2017 zu einer Arbeitsunfähigkeit führten, belegt die Depression mit 16,7 Prozent nach Muskel- und Skeletterkrankungen (21,8 Prozent) den zweiten Platz[2]. Depressionen zeigen sich zumeist in einer stark gedrückten Stimmung, der Betroffene ist in seiner Lebensqualität stark eingeschränkt. Nicht selten folgt darauf eine Abwärtsspirale, unter deren Auswirkungen nicht nur die berufliche Karriere, sondern auch das private Umfeld stark leiden. Wird einem depressiven Menschen länger nicht geholfen, kann es im Extremfall sogar zu Suiziden führen. Daher ist es umso wichtiger, dass Menschen in der Zeit zwischen Erstdiagnose und Therapie nicht alleine gelassen werden. Jede Hilfe ist willkommen – warum nicht auch eine App?

Neue Ansätze für die Unterstützung von Depressionen

Die Idee beim Einsatz von Wearables: Die in Frage kommenden Geräte messen zum einen kontinuierlich Vitalparameter wie Bewegung (Schritte), Herzschlag und Anspannung (Hautwiderstand), zum anderen gleichzeitig auch Umweltparameter wie beispielsweise Helligkeit, Luftfeuchtigkeit und lokale Pollendichte. Dunkelheit kann in Verbindung mit einer Belastung durch Pollen zur Verschlechterung des Zustands einer bereits depressiven Person führen. Gerade diese Kombination der erfassten Parameter macht das Projekt Selfpass so interessant. Die vielen Daten sollen künftig auch mit den Ansätzen der künstlichen Intelligenz ausgewertet werden. Ziel ist insbesondere die Gewinnung weiterer Erkenntnisse darüber, wie sich die Parameter gegenseitig beeinflussen. Patienten sind nach einer Herzerkrankung besonders anfällig für eine Depression. Einfache Atemübungen oder Meldungen wie zum Beispiel „Geh doch mal raus und genieß das Wetter", sind oft schon hilfreich – unter der Bedingung, dass

es draußen nicht regnet und auch kein starker Pollenflug herrscht. Weiter bietet die App Übungen und Aufgaben im Bereich der Planung und Konzentration, die dem Patienten helfen sollen.

Die Selfpass-Plattform begleitet die Patienten durch ihren gesamten Alltag. Eine automatische Auswertung von regelmäßigen Fragen mithilfe der App, gekoppelt mit der intelligenten Auswertung der Wearable-Messdaten gibt darüber Auskunft, wie der aktuelle Zustand des Patienten ist. Anhand dieser Messdaten werden selbstständig passende Übungen und Aufgaben für den Patienten ausgewählt, die im Laufe des Tages, auch mithilfe der App, zu erledigen sind.

Im Rahmen des Forschungsprojektes liegt ein besonderes Augenmerk auf IT-Sicherheit und Datenschutz bei den verwendeten Wearables. Dabei wurden bei den von den Wearable-Herstellern bereitgestellten Geräten die Datenschutzerklärungen untersucht und die Apps IT-Sicherheits-technisch analysiert. Auch bei der Umsetzung des (Cloud)-IT-Systems für die Verarbeitung von Daten, die zunächst Probanden und im späteren Verlauf des Projektes Patienten bereitgestellt werden, wurden Analysen durchgeführt. Die notwendigen Attribute der neuen Datenschutz-Grundverordnung (DS-GVO), die seit dem 25. Mai 2018 verpflichtend in Europa gültig ist, wurden sofort in Selfpass integriert. Nutzern muss es demnach unter anderem möglich sein, alle ihre personenbezogenen Daten in einem offenen Datenformat aus dem IT-System extrahieren zu können, um sie gegebenenfalls bei einem anderen Anbieter einzuspeisen. Zukünftig werden nach ersten Probandenstudien echte Patientendaten in die Selfpass-Platt-

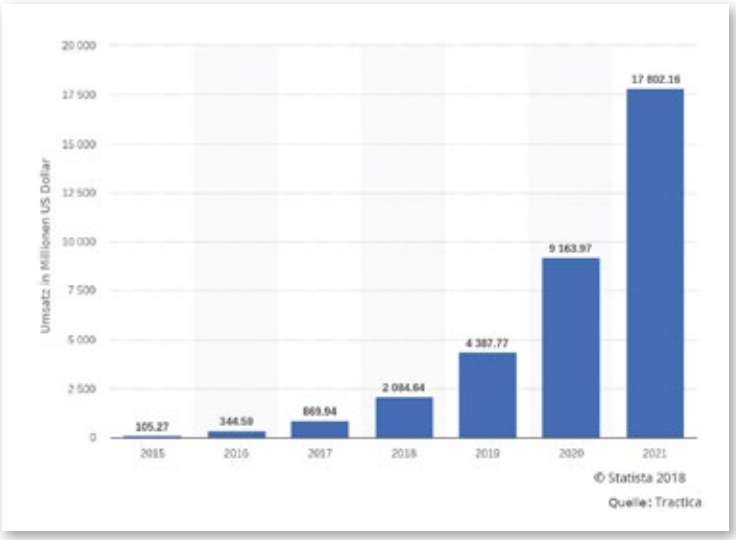

Abbildung 1: Weltweit geschätzter Umsatz für Wearables aus dem Bereich Healthcare von 2015 bis 2021.[3][4] (Quelle: tractica)

HINTERGRUND

Zusammen mit den Forschungspartnern aus dem Universitätsklinikum Heidelberg, der Technischen Universität Berlin und der Medisite GmbH arbeitet das Institut für Internet-Sicherheit – if(is) im Forschungsvorhaben „Self-administered Psycho-Therapy-Systems (Selfpass). In diesem Forschungsprojekt soll eine Plattorm entwickelt werden, die Patienten, bei denen in einem ersten Arztgespräch eine Depression diagnostiziert wurde, dabei hilft, die Zeit bis zu ihrer ersten Therapiesitzung zu überbrücken und langfristig zu begleiten. Die Plattform soll den Patienten dabei in seinem Alltag unterstützen und anhand von Messdaten der Wearable-Geräte erkennen, ob sich eine Depression verstärkt oder abnimmt und dementsprechend Therapiemaßnahmen einleiten.

Ein besonderer Fokus wird dabei insbesondere auf den Datenschutz und die Datensicherheit der Anwendung und der dahinter befindlichen IT-Infrastruktur gelegt. Gefördert wird das Projekt im Rahmen des Aktionsfeldes „Gesundheitswirtschaft im Rahmenprogramm Gesundheitsforschung“ durch das Bundesministerium für Bildung und Forschung (BMBF). Die Patienten sollen die Möglichkeit erhalten, durch eine Android- oder iOS-App ihren Zustand selbst zu prüfen, so dass es bei einer Verschlechterung die Möglichkeit gibt, mit einfachen Therapiemaßnahmen direkte Selbsthilfe anzubieten, beziehungsweise bei starken Verschlechterungen des Zustandes einen Kontakt zu einem Notfallteam anzubieten.

form eingepflegt. Hier handelt es sich um medizinische Daten, für die eine gesetzliche Aufbewahrungspflicht von bis zu 30 Jahren gilt. In dieser Zeit ist dementsprechend nur eine Sperrung der personenbezogenen Nutzerdaten möglich, gesperrte Daten dürfen dann nicht weiter verarbeitet werden.

Risikofaktoren bei dem Einsatz von Wearables

Der Markt für Wearables unterliegt bereits seit vielen Jahren einem starken Wachstum. Nahezu jeder Smartphone-Hersteller bietet auch eigene Wearables beziehungsweise Fitnessarmbänder an. Darüber hinaus gibt es Hersteller, die sich einzig und alleine auf Fitness Wearables spezialisiert haben. Der Markt wird laut einer Studie des Marktforschungsunternehmens tractica aus den USA alleine im Bereich der Gesundheits-Wearables von 2,1 auf 17,8 Milliarden US-Dollar wachsen.

IT-Sicherheit, Datenschutz und Präzision der Wearables

Im Rahmen des Projektes Selfpass konnte festgestellt werden, dass die Präzision einzelner Geräte sehr unterschiedlich ist. Es waren teils deutliche Unterschiede bei der Messung des Puls und der Zählung der Schritte zu verzeichnen. Auf dem Markt fehlen auch noch Geräte, die als Medizinprodukt zertifiziert sind und dem Datenschutz in Europa Folge leisten. Viele Geräte stammen aus den USA, Südkorea und China – oft ist der Datenschutz hier noch nicht angemessen umgesetzt. Die DS-GVO gilt allerdings auch für ausländische Unternehmen, wenn sie ihre Dienste in Europa anbieten.

Quellcodeanalyse der Applikationen

Im Rahmen von IT-Sicherheitsstudien wurden auch diverse Android-Apps analysiert. Für tiefergehende Untersuchungen wurden die Applikation zunächst dekompiliert, um eine verständliche Form, den Quellcode, für die Analyse nutzen zu können. Darauf aufbauend war es mit verschiedenen standardisierten Vorgehensweisen und Unterstützungs-Tools möglich, einen sehr detaillierten Einblick in die zu überprüfende App zu gewinnen.

Bei den Anwendungstests der Wearables wurden im Wesentlichen keine kritischen Sachverhalte identifiziert, die das direkte Zusammenspiel zwischen Benutzer und Applikation gefährden. Würde es jedoch einem Angreifer gelingen, eine manipulierte Version der getesteten Anwendungen auf das Gerät eines potenziellen Opfers zu schleusen, so wären anhand der identifizierten Schwachstellen einige Angriffsszenarien denkbar.

So wurde beispielsweise eine Schwachstelle bei mehreren Apps identifiziert, mit der es möglich wäre, Betriebssystemkommandos auszuführen. Bei dieser Attacke würden die vom Angreifer bereitgestellten Betriebssystembefehle mit den Rechten der anfälligen Anwendung ausgeführt. Damit dieser Angriff funktioniert, ist nach Abänderung des Quellcodes zusätzlich eine Neukompilierung notwendig. Erst nachdem diese Schritte abgeschlossen sind, kann die „Auslieferung" an das potenzielle Opfer stattfinden. In der Praxis wird ein solcher Angriff als „Command Injection" bezeichnet. Den Boden dafür bereiten unzureichende Eingabevalidierungen.

An anderer Stelle wurde eine Schwachstelle gefunden, welche es einem Angreifer erlaubt, Abfragen auf die verwendete Datenbank der App abzusetzen. Dies ist möglich, da im Quellcode native, hart codierte SQL-Abfragen ausgeführt werden. Ein Angreifer könnte diese Abfragen nun beliebig anpassen, um aus der Datenbank vertrauliche Informationen zu extrahieren. Um diese Art von Schwachstelle zu verhindern, sollten alle sensiblen Informationen der Datenbank verschlüsselt und lediglich systemintern verarbeitet werden.

Wie bereits bei der Command-Injection-Schwachstelle ist auch hier eine Neukompilierung der App erforderlich, sowie die anschließende Auslieferung an das Opfer. Aus diesem Grund besteht für einen Benutzer der App zunächst keine Gefahr, solange Apps lediglich von vertrauenswürdigen Quellen installiert werden. Aus rein programmiertechnischer Sicht bleiben die identifizierten Mängel jedoch weiter als kritisch einzustufen.

Angriffsvektoren bei Wearables

Im IT-Umfeld eines Fitness-Armbandes beziehungsweise einer Smartwatch haben

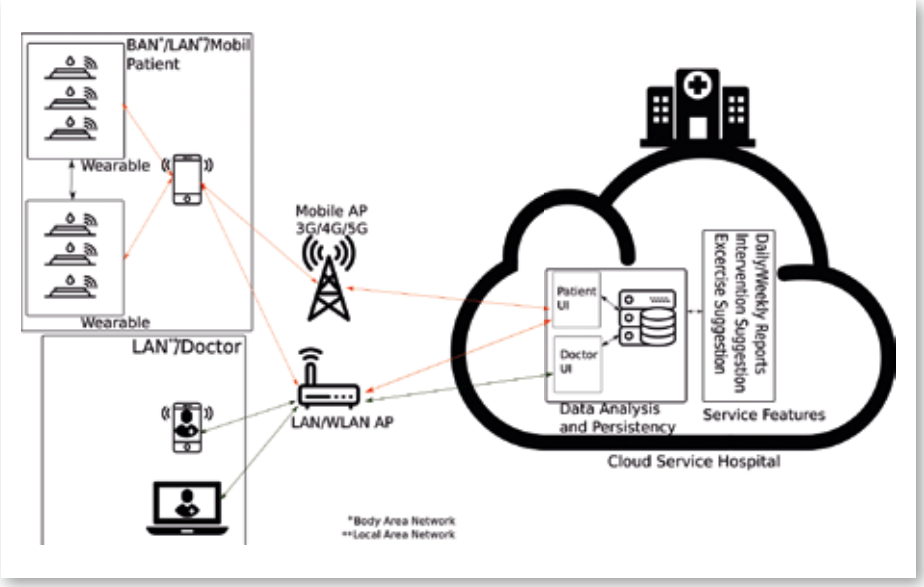

Abbildung 2: Skizzierung einer Cloud-Umgebung im Umfeld von Selfpass

sich als Luftschnittstellen drei Kommunikationsstandards etabliert: Bluetooth ist die häufigste Verbindungsart, gefolgt von WLAN und dem Mobilfunk, einschließlich seiner Übertragungsstandards 3G (HSDPA), 4G (LTE) und zukünftig auch 5G. Nutzt ein Wearable ausschließlich Bluetooth, dient das Smartphone als zentraler Verbindungspunkt, in dem alle Daten mithilfe der dementsprechenden App gespeichert werden. Bei WLAN-fähigen Wearables ist dies ganz ähnlich, jedoch können Daten direkt in die Cloud zum jeweiligen Anbieter übermittelt werden. Unterstützt das Gerät Mobilfunkverbindungen, kann die Smartwatch sogar als Smartphone Ersatz dienen: Je nach Gestaltung lassen sich Anrufe tätigen, E-Mails austauschen und Web-Verbindungen herstellen.

All dies bringt potenzielle Risiken mit sich, die dementsprechend auch eine breitere Angriffsfläche für Angreifer darstellen und höhere Sicherheitsanforderungen an ein Wearable stellen. Untersuchungen haben bei ausgewählten Smartwatches und Fitness-Armbändern festgestellt, dass das Sicherheitsbewusstsein bei den bekannten Herstellern in einem höherwertigen Preissegment in den letzten Jahren deutlich gestiegen ist. Es sind keine unverschlüsselten Verbindungen mehr zu finden. Auch wird immer häufiger das so genannte HTTP Public Key Pinning verwendet, das wirksam gegen Man-in-the-Middle-Angriffe schützt. Dabei werden Signaturen der Zertifikate auf den jeweiligen Geräten geprüft. Somit ist es unbekannten Dritten nicht mehr möglich, durch selbst erstellte TLS-Zertifikate, verschlüsselte Verbindungen vorzutäuschen und somit Nutzerinformationen abzugreifen. Deutliche Schwachstellen wurden bei der Ausstellung der serverseitigen TLS-Zertifikate entdeckt, die immer noch mit dem als zu schwach angesehenen Signierungsalorithmus SHA-1 erfolgt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) weist in seiner technischen Richtlinie zu kryptographischen Verfahren darauf hin, auf die Nutzung von SHA-256 beziehungsweise auf SHA-384 umzustellen und somit potenzielle Risiken bezüglich SHA-1 auszuschließen.

Abbildung 3: Verbindungsinformationen für ein Fitness-Armband von Garmin.

Kommunikationsverhalten der Android-Apps

Im Rahmen des Projekts wurde auch das Kommunikationsverhalten der einzelnen Wearables und der dazugehörigen Smartphone Apps untersucht. Dabei wurde insbesondere darauf geachtet, wohin die einzelnen Geräte die aufgezeichneten Nutzerdaten senden. Die Wearables selbst kommunizieren lediglich mit diesen Apps und diese senden dann wiederum Daten an andere Server.

Es wurde ein Analyse-System genutzt, das im Hintergrund untersucht, wohin die Applikationen, die auf dem Smartphone gerade aktiv sind, Daten senden[5]. Im Rahmen des Projektes wurden ausschließlich Android-Anwendungen untersucht. Es wurden sämtliche Datenpakete mitgeschnitten, die das Smartphone empfängt und versendet.

Auf dem für diese Untersuchung genutzten Test-Smartphone wurden schließlich die ausgewählten Apps installiert. Anschließend wurde das Smartphone mit jeweils einem Wearable für fünf Tage gekoppelt und getestet. Dies geschah für alle Wearables und nach der Testzeit wurden die Verbindungsdaten von allen Geräten ausgewertet.

Diese Verbindungsdaten beinhalteten IP-Adressen, an die die jeweiligen Applikationen Daten gesendet haben. Der nächste Schritt der Auswertung bestand darin, zu ermitteln woher diese IP-Adressen stammen. Jeder IP musste ein geografischer Standort

Gerät	Anzahl an Verbindungen	Verbindungen, die ausschließlich starke Cipher-Suiten nutzen
Fitbit Blaze	33	3
Garmin Vivoactive HR	25	0
Microsoft Band 2	11	0
Polar A360	4	0
Runtastic Orbit	40	10
Samsung Gear Fit 2	31	10

Tabelle: Ergebnisse der Verbindungsanalyse im Hinblick auf die unterstützten Cipher Suiten.

zugeordnet werden, um herauszufinden, wo die jeweiligen Server stehen, welche die Daten der Applikation empfangen.

Die Hauptergebnisse der Analyse zeigten, dass sämtliche Geräte Daten an diverse Standorte schicken. Darüber hinaus senden alle Wearables Daten auch an Server außerhalb Europas, konkreter an Server in den USA. Da in den USA der Zugriff auf die Daten gesetzlich anders als in Europa geregelt ist, wird eine Speicherung von persönlichen Daten in den USA als kritisch betrachtet. Zusätzlich wurden die Server, an die Daten gesendet wurden, einer ersten sicherheitstechnischen Untersuchung unterzogen.

Es wurde insbesondere auch analysiert, welche Kryptographie-Methoden (Cipher Suiten) von den Smartphones angeboten und von den verschiedenen Servern für die SSL/TSL-Verbindung ausgewählt wurden. Die ausgewählte Cipher Suite beschreibt, welche Algorithmen für den Schlüsselaustausch, die Verschlüsselung und die Authentifizierung genutzt werden.

Die Ergebnisse dieser Auswertung zeigten, dass nur ein Bruchteil der Server, an die Daten gesendet werden, ausschließlich starke Cipher Suiten auswählt (siehe Tabelle). Bei allen anderen werden auch noch Algorithmen akzeptiert, die als schwach gelten und damit ein Sicherheitsrisiko darstellen können.

Die Kommunikationsanalyse macht deutlich, dass Wearables die persönlichen Daten der Nutzer an eine Vielzahl von Orten auf der ganzen Welt schicken. Dabei hat der normale Nutzer keinen Überblick darüber, was mit seinen Daten geschieht.

Fazit

Mit dem Verbundvorhaben Selfpass wird aktuell eine sehr fortschrittliche und sichere Anwendung zur Unterstützung bei Depressionserkrankungen entwickelt. Die Erkenntnisse aus den dabei entdeckten Sicherheitsmängeln bei Android-Apps in Kombination mit Erkenntnissen aus den Datenschutzanalysen fließen direkt in die Weiterentwicklung ein. Ziel ist, die Selfpass-Anwendung möglichst robust zu gestalten und ein Höchstmaß an IT-Sicherheit und Datenschutz zu bieten.

Auf dem Markt der Wearables ist festzustellen, dass es an präzisen Geräten, insbesondere solchen aus Europa, schwer mangelt. Nur im europäischen Wirtschaftsraum kann ein hoher gesetzlicher Standard bei dem sensiblen Thema Datenschutz gewährleistet werden. Positiv ist jedoch auch anzumerken, dass die hier analysierte Stichprobe der Android-Anwendungen auf den Übertragungswegen grundsätzlich die Daten verschlüsseln. Dies ist jedoch auch den Weiterentwicklungen und höheren Sicherheitsrichtlinien bei der Entwicklung von Android-Apps selbst zu verdanken. Entwicklern werden viele einfache Möglichkeiten geboten, ein ausreichendes Maß an Sicherheit in moderne Anwendungen zu integrieren. Über das serverseitige Umfeld bei den Anbietern der Wearable-Anwendungen selbst kann bis auf die Analyse der Verschlüsselungsstärken und die Aufzeichnung der vielen unterschiedlichen IP-Verbindungen keine weitere Aussage getroffen werden. Nutzer geben mit Smart-Watches, Fitness-Armbändern oder Gesundheitsarmbändern viele sensible Informationen über sich preis. Das werden sie langfristig nur tun, wenn die IT-Systeme diese sicher und vertrauenswürdig verarbeiten. ■

Referenzen:

[1] statista, „Arbeitsunfähigkeitstage aufgrund psychischer Erkrankungen in Deutschland", https://de.statista.com/statistik/daten/studie/254194/umfrage/au-tage-aufgrund-psychischer-erkrankungen-in-deutschland-nach-geschlecht/, [Zugriff am 19.06.2018]

[2] statista, „Anteile der zehn wichtigsten Krankheitsarten an den Arbeitsunfähigkeitstagen in Deutschland", https://de.statista.com/statistik/daten/studie/77239/umfrage/krankheit---hauptursachen-fuer-arbeitsunfaehigkeit/, [Zugriff am 19.06.2018]

[3] statista, "Projected size of the global market for wearable devices in the healthcare sector " https://www.statista.com/statistics/607982/healthcare-wearable-device-revenue-worldwide-projection/, [Zugriff am 19.06.2018]

[4] Tractica, Wearable Devices for Healthcare Markets, https://www.tractica.com/research/wearable-devices-for-healthcare-markets/, [Zugriff am 19.06.2018]

[5] Fischer, Janosch: „Analyse des Kommunikationsverhaltens von Android-Apps", Bachelor Arbeit 2013, Computer Networks Research Group, Cologne University of Applied Sciences, Prof. Dr. A. Grebe, in Kooperation mit Prof. Dr. C. Vogt

FALK GAENTZSCH,
wissenschaftlicher Mitarbeiter und Projektleiter am Institut für Internet-Sicherheit – if(is) der Westfälischen Hochschule Gelsenkirchen

JANOSCH FISCHER,
wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit – if(is) der Westfälischen Hochschule Gelsenkirchen

PROF. DR. NORBERT POHLMANN
ist Professor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.