Unter Smart Health versteht man elektronikbasierte Diagnose- und Behandlungssysteme (z. B. Blutdruckmessgerät, Waage, Thermometer), spezielle Sensoren (z. B. Fallsensoren, Sensoren in der Toilette, Wärmesensoren), Wearables (z. B. Smartwatches, Fitness-Tracker oder Smartphones) bis hin zu intelligenten Körpermodifikationen (z. B. Implantate oder Prothesen), die miteinander verbunden sind. Durch die Vernetzung dieser und die Kombination mehrerer solcher Gegenstände werden neue Funktionen und Dienste möglich, die gegenüber dem einzelnen Gegenstand einen Mehrgewinn bieten. Die Geräte der Diagnose/Behandlung/Sensorik können oft mit einem weiteren Gerät z. B. Wearables oder Smartphone verbunden werden und dadurch zusätzlich gesteuert werden.

Diese neue Technologie bringt eine Reihe von Verbesserungen mit sich:

- Verbesserte Information für den Arzt z. B. bei Blutdruckmessgeräten durch Messung und Übertragung
- Verbesserte Gesundheit z. B. bei Fitness-Trackern durch Analyse des Schlafs
- Verbesserte Notfallversorgung z. B. bei Fallsensoren durch direkte Notfallnachricht an Rettungsdienst

Viele Nutzer gehen davon aus, dass Ihre Geräte bereits per Default – also vor dem Kauf – vom Hersteller bezüglich des Schutzes Ihrer Privatsphäre bzw. Sicherheit eingestellt werden. Nicht jeder Hersteller hat aber ein Interesse daran, dass die Geräte zum maximalen Schutz der Privatsphäre eingestellt werden. Zum einen sind manche Hersteller an den zusätzlichen Daten interessiert. Zum anderen geht maximale Privatsphäre bzw. Sicherheit manchmal mit Einbußen in der Funktionalität einher. Da man vorher nicht weiß, wie die Einstellung des Herstellers zum Thema Privatsphäre bzw. Sicherheit ist, sollte man sich bei der Konfiguration mit den Einstellungen beschäftigen. Nur so kann sichergestellt sein, dass die eigenen Präferenzen gewährleistet werden.
Deshalb ist es wichtig, dass Sie sich bei der Konfiguration Ihres Smart Health-Geräts ausreichend Zeit nehmen, um die Konfiguration hinsichtlich Sicherheit und Privatsphäre durchzuführen. Außerdem sollten Sie während der Nutzung der Smart Health-Geräte etwaige auftretende Meldungen sorgfältig lesen und entsprechend der Handlungshinweise handeln.

All dies sind Beispiele, die bereits in der Praxis aufgetreten sind. Das Gefährliche beim Sammeln und Auswerten von Daten und Informationen über das eigene Nutzungsverhalten ist, dass heute noch nicht absehbar ist, was künftig alles aus den Daten abgeleitet werden kann, z. B. welche Krankheiten eine Person hat oder der Wahrheitsgehalt von Aussagen, die Sie anderen Menschen gegenüber machen.

Kontakt

Karlsruhe Institut für Technologie (KIT)

Institut für Angewandte Informatik und
Formale Beschreibungsverfahren (AIFB)

Forschungsgruppe Security • Usability • Society (SECUSO)

Prof. Dr. Melanie Volkamer
Kaiserstraße 89, Gbd. 05.20
76133 Karlsruhe

Telefon: +49 721 608 450 45
E-Mail: kontakt@secuso.org

www.secuso.aifb.kit.edu
facebook.com/secuso
twitter.com/secusoresearch

Herausgeber

Karlsruher Institut für Technologie (KIT)

Präsident Professor Dr.-Ing. Holger Hanselka
Kaiserstraße 12
76131 Karlsruhe
www.kit.edu

Dieser Inhalt wurde im Europäischen Union Horizon 2020 Forschungs- und Innovationsprogramm unter der Zuwendungsvereinbarung Nr. 740923, Projekt GHOST (Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control) entwickelt.

Karlsruher Institut für Technologie

aifb

Smart Health

Mehr über Sicherheits- und Privatsphärenrisiken erfahren

INSTITUT FÜR ANGEWANDTE INFORMATIK UND FORMALE BESCHREIBUNGSVERFAHREN (AIFB)

SECUSO
SECURITY · USABILITY · SOCIETY

KASTEL

In diesem Faltblatt erhalten Sie Informationen über Sicherheits- und Privatsphärerisiken bzw. deren Konsequenzen.

Sicherheitsrisiken

Hacker können Ihnen auf vielfältige Art und Weise schaden: Wenn Hacker sich Zugriff auf Ihre Smart Health-Geräte verschafft haben, können diese Daten und Informationen, die in den Geräten hinterlegt oder mit diesen erzeugt werden, ausspähen.

Darüber hinaus können Hacker Ihre Smart Health-Geräte dann kontrollieren und auch umkonfigurieren und so z. B.

- Kontrolle über Sensoren übernehmen (dadurch können z. B. sensible Daten wie Blutdruck oder Puls jederzeit von Ihnen erfasst und an den Angreifer geschickt werden),
- den Arzt veranlassen, die Medikation zu verändern (weil die Gesundheitsdaten geschönt oder verschlechtert wurden),
- Diagnosegeräteeinstellungen verändern (dadurch leiden z. B. die kontinuierlichen Profile Ihrer Gesundheitsdaten),
- Daten der Sensoren umprogrammieren (dadurch senden z. B. die Fallsensoren ein irrtümliches Notfallsignal),
- Wearables manipulieren (dadurch werden z. B. ohne Grund Notruf-Signale abgesendet),
- Toilettensensoren überlasten (dadurch wird z. B. Ihre Toilette zerstört oder Ihre Wasserrechnung erhöht),
- verbundenen Implantate oder Prothesen manipulieren (dadurch wird die Lebensdauer verringert oder die Körpermodifikationen können sogar zerstört werden),
- Kontrolle über Fernwartung der Geräte übernehmen (dadurch können z. B. Geräte ein-/ausgeschaltet werden und zu lebensbedrohlichen Situationen führen).

Privatsphärenrisiken

Die Hersteller der Smart Health-Geräte sammeln eine Vielzahl von Daten und Informationen, z. B. Schlafzeiten, Puls, Blutdruck, Sportaktivität, Gewicht oder Informationen über Bewegungen. Manchmal werden nachträglich durch ein Update, Funktionen aktiviert, die Ihre Daten in Zukunft erheben. Die Zustimmung zu diesen zusätzlichen Daten versteckt sich manchmal tief in den neuen Vereinbarungen und ist nicht immer klar erkenntlich.

Ihre Nutzungsgewohnheiten werden aus diesen Daten abgeleitet (z. B. an welchen Tagen Sie sich zu welchen Uhrzeiten sportlich betätigt haben, zu welchen Uhrzeiten an welchen Tagen Sie ins Bett gegangen sind, Veränderungsverläufe Ihres Gewichts). So können die Hersteller umfangreiche Nutzungsprofile von Ihnen erstellen. Diese werden von den Herstellern Ihrer Geräte oder den App-Herstellern auf Ihren Geräten u. a. dafür verwendet, die Dienste zu verbessern oder zur Fernwartung der Geräte/Services.

Wenn die gesammelten Daten und die erstellten Nutzungsprofile allerdings in die Hände Dritter geraten oder von dem Hersteller entgegen der Vereinbarung für weitere Zwecke verwendet werden, kann Ihnen auf vielfältige Art und Weise Schaden entstehen.

Beispiele für konkrete Konsequenzen:

Die Informationen aus der Kombination von verschiedenen Profilen (z. B. Sportaktivität und Schlafzeiten) können, wenn sie bei Dritten landen, genutzt werden, um gezielt Einbrüche durchzuführen.

Ihre Gesundheitsdaten (z. B. Krankenakte, aktuelle Blutdruckwerte, einzunehmende Medikamente) können, wenn sie an Ihren derzeitigen oder potenziellen Arbeitgeber weitergegeben werden, dazu führen, dass Sie schlechtere Chancen bei der Bewerbung auf einen neuen Job haben oder dass Sie gekündigt werden.

Ihre Gesundheitsdaten können, wenn sie an Versicherungen weitergegeben werden, dazu führen, dass Ihnen keine Versicherung angeboten wird oder zu schlechteren Konditionen.

Ihre Gesundheitsdaten können, wenn sie an Ihre Bank weitergegeben werden, dazu führen, dass Sie schlechtere Konditionen für einen Kredit erhalten.

Die Kombination von Ihren Gesundheitsdaten (z. B. der Cholesterinspiegel) und ihre sportliche Aktivität können an Ihre Versicherung weitergegeben werden. Sie können dann dazu genutzt werden, um Sie in der Gestaltung Ihres Lebens einzuschränken, wenn Sie nicht in einen schlechteren Tarif eingestuft werden möchten.

Ihre allgemeinen personenbezogenen Daten (z. B. Namen, Adresse, Geschlecht oder Bankdaten) können, wenn sie bei Dritten landen und zu einem Profil verknüpft werden, genutzt werden, um Ihre digitale Identität zu übernehmen und unangemessene Inhalte in Ihrem Namen zu veröffentlichen, gefährliche Nachrichten (z. B. Phishing Nachrichten oder Nachrichten mit gefährlichen Anhängen) in Ihrem Namen zu verschicken oder finanzielle Transaktionen in Ihrem Namen durchzuführen.

Ihre Fitness-, Gesundheits- und Sensordaten können, wenn sie bei Dritten laden, dazu führen, dass Sie sich nicht mehr ungestört in Ihrem Heim fühlen. Dadurch können Sie sich selbst in Ihren Tätigkeiten/Verhalten einschränken oder eingeschränkt fühlen.

Dritte kommen an diese Daten, Informationen bzw. Nutzungsprofile entweder, weil

- Sie dem Hersteller der Smart Health-Geräte oder der App dies explizit (ggf. unbewusst) erlaubt haben.
- Sich kriminelle Mitarbeiter beim Hersteller finanziell bereichern möchten und daher die Daten unerlaubterweise kopieren und an Dritte weitergeben bzw. verkaufen.
- Hacker Sicherheitslücken in den Systemen und/oder Servern der Hersteller ausnutzen und sich so Zugriff auf die Daten, Informationen bzw. Nutzungsprofile verschaffen. Dann können Hacker diese selbst nutzen, um Ihnen zu schaden, sie veröffentlichen oder Sie damit erpressen, dass sie diese Daten, Informationen und Nutzungsprofile veröffentlichen oder sie an Dritte verkaufen.