Unter Smart Health versteht man eine Vielzahl von Geräten bzw. Gegenständen, die im eigenen Haus oder der eigenen Wohnung verwendet werden, die untereinander kommunizieren können und mit dem Internet verbunden sind. Die Liste möglicher Geräte umfasst:

- Elektronikbasierte Diagnose- und Behandlungssysteme: z. B. Blutdruckmessgeräte, Waagen, Thermometer;
- Spezielle Sensoren: z. B. Fallsensoren, Sensoren in der Toilette, Wärmesensoren;
- Sogenannte Wearables: z. B. Smartwatches, Fitness-Tracker oder Smartphones;
- Intelligente 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.

Smart Health Anwendungen bringen daher eine Reihe von Verbesserungen mit sich:

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

Studien zeigen, dass viele Nutzer von Smart Health Geräten und Anwendungen davon ausgehen, dass Ihre Geräte bereits per Default – also vor dem Kauf – maximalen Schutz Ihrer Privatsphäre bzw. Sicherheit bieten. Diese Annahme ist aus folgenden Gründen problematisch:
Es gibt Hersteller, die gar keinen maximalen Schutz bieten wollen oder nicht in der Lage sind diesen zu gewährleisten: z. B.

- sind manche Hersteller an den zusätzlichen Daten, die erhoben werden, interessiert, um diese gewinnbringend zu verkaufen;
- haben sich manche Hersteller bewusst dagegen entschieden, einen möglichst guten Schutz zu bieten, denn maximale Privatsphäre bzw. Sicherheit geht mit hohen Kosten sowie mit Einbußen in der Funktionalität einher;
- sind manche Hersteller zwar motiviert einen möglichst hohen Schutz zu bieten, aber sind wegen der Komplexität der Infrastruktur und den Möglichkeiten des Angreifers gar nicht in der Lage, dies zu leisten.

Hier erfahren Sie welche Risiken für Ihre Sicherheit und Ihre Privatsphäre bei der Nutzung von Smart Health Geräten und Anwendungen bestehen.

Kontakt

Karlsruher 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

secuso.aifb.kit.edu
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

Sicherheit und Privatsphäre können auf unterschiedliche Arten gefährdet werden. Im Folgen werden die unterschiedlichen Risiken erläutert:

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),
- verbundene 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. Dies ist im besten Fall alles notwendig, um die gewünschte Funktionalität zu bieten. Ihre Nutzungsgewohnheiten können aber auch aus diesen Daten abgeleitet werden (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 im besten Fall von den Herstellern Ihrer Geräte bzw. Ihrer Smart Health Anwendungen dafür verwendet, die Dienste zu verbessern oder zur Fernwartung der Geräte bzw. Dienste und Anwendungen.

Wenn die gesammelten Daten und die erstellten Nutzungsprofile allerdings in die Hände Dritter geraten (z. B. weil Kriminelle sich in die Systeme des Herstellers hacken i. d. R. weil diese nicht ausreichend geschützt sind) oder von dem Hersteller entgegen Ihrer Erwartungen für weitere Zwecke verwendet werden, kann Ihnen auf vielfältige Art und Weise Schaden entstehen.

Beispiele hierfür sind:

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.

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

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 landen, 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.

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.