Fitness-Tracker schwächeln

Informatiker der TU Darmstadt decken schwere Sicherheitsmängel auf

Kommunikation und Medien
Corporate Communications

Karolinenplatz 5
64289 Darmstadt

Ihre Ansprechpartnerin:
Simone Eisenhuth
Tel. 06151 16 - 21426
Fax 06151 16 - 23750
eisenhuth.si@pvw.tu-darmstadt.de

www.tu-darmstadt.de/presse
presse@tu-darmstadt.de

Darmstadt, 9. September 2016. Sie sehen oft aus wie eine Armbanduhr, können aber viel mehr als nur die Zeit anzeigen. Sogenannte Fitness-Tracker sammeln im großen Stil Informationen über die Lebensweise und den Gesundheitsstatus ihrer Nutzer, um ihnen beispielsweise beim Trainieren oder Abnehmen zu helfen. Die Datensicherheit der Alltagshelfer überprüften Ahmad-Reza Sadeghi, Professor für Systemsicherheit am Profilbereich Cybersecurity (CYSEC) der TU Darmstadt, und sein Team – mit alarmierenden Ergebnissen.

Die Beliebtheit und Verbreitung von Fitness-Trackern nimmt immer weiter zu. Allein im ersten Quartal 2016 wurden weltweit knapp 20 Millionen solcher Tracker verkauft [1]. Viele zeichnen per GPS die gelaufenen Kilometer auf, können Herzfrequenz und Puls messen oder feststellen, ob der Träger oder die Trägerin schläft. „Zunehmend werden diese Daten nicht für den ursprünglichen Zweck, sondern von Dritten verwendet“, erklärt Professor Sadeghi.

In den USA werden Daten von Fitness-Trackern vor Gericht bereits als Beweismittel zugelassen, wie das Forbes Magazine schon 2014 berichtete [2]. Die Geräte würden von Polizisten und Juristen als „Black Box“ des menschlichen Körpers angesehen, schrieb die NY Daily News 2016 [3]. Und manche Krankenversicherungen bieten seit neuestem Rabatte an, wenn die Kunden dafür Daten ihrer Fitness-Tracker zur Verfügung stellen. Das locke Betrüger an, die die aufgezeichneten Daten verändern, um sich finanzielle Vorteile zu erschleichen oder gar einen Gerichtsprozess zu manipulieren, so Sadeghi. Umso wichtiger sei es, dass das Übertragen, Verarbeiten und Speichern der sensiblen persönlichen Daten hohen Sicherheitsstandards genügt.

Leichtes Spiel für Angreifer

Um das zu überprüfen, führten Sadeghi und sein Team in Kooperation mit der Universität Padua, Italien, eine Studie mit 17 unterschiedlichen Fitness-Trackern durch, sowohl von weniger bekannten Herstellern als auch von beliebten Marken wie Xiaomi, Garmin und Jawbone. Die Forscher konzentrierten sich darauf, die an den Server gesendeten Daten durch einen „Man-in-the-Middle“-Angriff zu manipulieren und untersuchten dabei die Sicherheit der verwendeten Kommunikationsprotokolle.

Das Ergebnis: Zwar sichern alle cloud-basierten Tracking-Systeme die Datenübertragung mit dem verschlüsselten Protokoll HTTPS. Trotzdem gelang es den Forschern in allen Fällen, die aufgezeichneten Daten zu manipulieren. Von den untersuchten Fitness-Trackern nutzen die meisten keine Schutzmechanismen, nur vier Hersteller verwenden geringfügige Maßnahmen zum Schutz der Integrität – also der Unversehrtheit und Unverändertheit – der Daten. „Diese Hürden können einen motivierten Angreifer nicht aufhalten. Schon mit wenigen Vorkenntnissen wäre es Betrügern möglich, die Daten zu verfälschen“, warnt Sadeghi, da weder Ende-zu-Ende-Verschlüsselung noch ein sonstiger Manipulationsschutz während der Datenübertragung verwendet werde.

Fünf der untersuchten Geräte synchronisieren die Fitness-Daten nicht mit einem Online-Dienst. Allerdings speichern die Hersteller die Daten im Klartext, also unverschlüsselt und für jeden lesbar, auf dem Smartphone – sobald dieses gestohlen oder mit einer Schadsoftware infiziert wird, können die Daten unautorisiert weitergegeben und manipuliert werden. Ein weiteres Sicherheitsrisiko von Fitness-Trackern, das die Cybersecurity-Experten der TU Darmstadt in ihrer Studie gefunden haben.

„Alle Versicherungen und auch andere Dienstleister, die Fitness-Tracker einsetzen wollen, sollten sich vorher mit Sicherheitsexperten beraten“, empfiehlt Sadeghi. Die in der Studie gefundenen Mängel seien mit bereits bekannten Standardtechnologien zu beheben, „die Hersteller müssten sich nur etwas mehr Mühe geben, diese auch in die Produkte zu integrieren“.

Weitere Informationen: Profilbereich CYSEC

CYSEC (Cybersecurity) ist ein Profilbereich der TU Darmstadt und Partner am Center for Research in Security and Privacy (CRISP). Das vom Bundesministerium für Bildung und Forschung (BMBF) und vom Land Hessen seit 2015 geförderte Kompetenzzentrum CRISP ist der größte Zusammenschluss von Forschungseinrichtungen im Bereich Cybersicherheit in Europa. Neben der TU Darmstadt sind auch die Hochschule Darmstadt, das Fraunhofer Institut für Sichere Informationstechnologie (SIT) und das Fraunhofer Institut für Graphische Datenverarbeitung (IGD) an CRISP beteiligt.

[1] http://bit.ly/1YmK6hK
[2] http://bit.ly/2cbLwb8
[3] http://nydn.us/2cHc3OP

TECHNISCHE UNIVERSITÄT DARMSTADT

Hinweis an die Redaktionen

Grafiken zu der Studie können unter www.tu-darmstadt.de/pressebilder heruntergeladen werden.

Ansprechpartner

Kontakt zu den Wissenschaftlern vermittelt (gerne auch an diesem Wochenende):

Ann-Kathrin Braun
CYSEC, TU Darmstadt
E-Mail: akbraun@cysec.tu-darmstadt.de
Mobil: +49 170 85 233 85

MI-Nr. 62/2016, Braun/se