



WEARABLES UND FITNESS-APPS: DATEN AUßER KONTROLLE



Smartwatches, Fitnessarmbänder und Fitness-Apps – der Boom rund um Wearables und Fitness-Apps hält an. Die smarten Alltagsbegleiter zählen schon längst nicht bloß die Schritte ihrer Nutzer: Sie wissen etwa, wie lange und wie gut ihre Träger schlafen, haben ihren Puls und Kalorienverbrauch im Blick und wissen, ob sie sich viel bewegen oder nicht. All das sind sensible Daten, die weitreichende Rückschlüsse auf Fitness und Gesundheit von Verbrauchern zulassen. Aber was passiert mit den gesammelten Daten? Haben Nutzer noch die Kontrolle?

Die Verbraucherzentrale NRW hat im Rahmen des Projekts Marktwächter Digitale Welt zwölf Wearables und 24 Fitness-Apps untersucht: Welche Daten erheben die Geräte und Apps eigentlich? An welche Server werden sie gesendet und wie sicher ist die Datenübertragung vor ungewolltem Zugriff? Wie gehen Anbieter mit geltenden Datenschutzbestimmungen um? Zusätzlich wurden auch Verbraucher befragt: Die Ergebnisse der repräsentativen Befragung zeigen, dass Datenschutz im Zusammenhang mit Wearables und Fitness-Apps auch ein wichtiges Thema für Verbraucher ist.

Ergebnisse der repräsentativen Verbraucherbefragung

...❖ DATENSCHUTZBEDENKEN: VERBRAUCHER BEFÜRCHTEN KONTROLLVERLUST

Sowohl Wearable-Nutzer als auch Nicht-Nutzer zeigen sich mehrheitlich besorgt, was den Umgang mit ihren online gesammelten Daten angeht und stören sich daran, die Kontrolle über ihre eigenen Daten abzugeben. Mögliche Folgen der Wearable-Nutzung werden jedoch unterschiedlich bewertet: Vergleichsweise viele Verbraucher fänden es beispielsweise akzeptabel, wenn Wearable-Daten etwa zur Überprüfung von Zeugenaussagen (61 %) oder im Rahmen von Arbeitgeber-Bonusprogrammen (44 %) verwendet würden. Die Erhöhung des eigenen Krankenkassentarifs auf Basis von Fitness-Daten würde wiederum nur ein kleinerer Teil der Befragten akzeptieren (13 %).

Ergebnisse der technischen Prüfung

...❖ DATEN AUSSER KONTROLLE

Die technische Prüfung von zwölf Wearables und 24 Fitness-Apps zeigt, dass eine Kontrolle über die eigenen Daten kaum möglich ist: Die Mehrzahl der Apps sendet – wenig datensparsam – zahlreiche, mitunter sensible Informationen an Anbieter-Server und bindet darüber hinaus auch Drittanbieter (z.B. Analyse-/Werbedienste) ein. So werden etwa technische Daten (z.B. Betriebssystem des Smartphones) von 16 der 19¹ Apps schon an Drittanbieter gesendet, bevor Verbraucher überhaupt den Nutzungsbedingungen zustimmen und über den Umgang mit ihren

Daten informiert werden konnten. Positiv ist, dass alle – von den untersuchten Fitness-Apps ausgehenden – Informationen https-transportverschlüsselt versendet werden. Aber: Nur wenige der untersuchten Wearables² sind vor ungewollter Standortverfolgung (Tracking) geschützt, was beispielsweise das Erstellen von Bewegungsprofilen möglich macht.

Ergebnisse der rechtlichen Prüfung³

...❖ MÄNGEL BEIM UMGANG MIT NUTZER-DATEN: ANBIETER LASSEN KUNDEN IM UNKLAREN

Anbieter müssen ihre Kunden darüber aufklären, wie sie mit den gesammelten Daten umgehen. Die Marktwächterexperten kommen zu der Einschätzung, dass dieser Informationspflicht in mehreren der untersuchten Fälle nicht ausreichend nachgekommen wird: Drei Anbieter stellen ihre Datenschutzhinweise nur in englischer Sprache bereit, nur zwei Anbieter informieren über die Besonderheit der erhobenen Gesundheitsdaten. Auch holt nur ein Anbieter eine separate Einwilligung für die Verarbeitung dieser sensiblen Gesundheitsdaten von den Nutzern ein. Fünf Anbieter halten es sich offen, die personenbezogenen Daten ihrer Nutzer bei Fusion oder Übernahme weiterzureichen. Darüber hinaus lässt die Textanalyse darauf schließen, dass die Datenschutzhinweise allesamt für den Verbraucher schwer verständlich sind.

Fazit der Untersuchung

...❖ VERBRAUCHERSORGEN SIND BEGRÜNDET

Die Ergebnisse der technischen und rechtlichen Prüfung zeigen, dass die Verbrauchersorgen begründet sind: Lückenhafter Schutz gegen ungewolltes Tracking, ein ausgeprägtes Datensendungsverhalten der Fitness-Apps und mangelnde Kontrollmöglichkeiten seitens des Nutzers zeigen, dass in Sachen Datenschutz und Datensicherheit nachgebessert werden muss.

¹ 19 von 24 Apps binden Drittanbieter mit ein.

² Bei inaktiver Kopplung, d.h. die Verbindung zwischen Wearable und Smartphone ist unterbrochen.

³ Die Datenschutzerklärungen wurden am 5. September 2016 zuletzt abgerufen. Aktualisierungen, die ggf. nach diesem Datum durch Anbieter vorgenommen wurden, waren nicht Bestandteil der Prüfung.

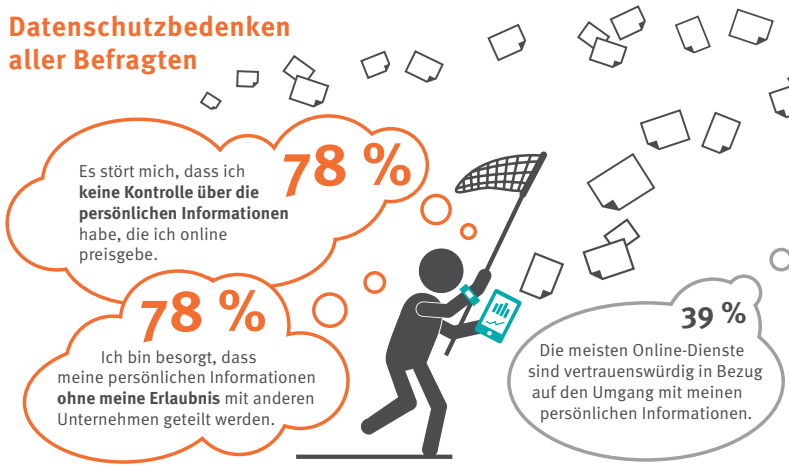
WEARABLES UND FITNESS-APPS

DATENSCHUTZBEDENKEN: VERBRAUCHER BEFÜRCHTEN KONTROLLVERLUST



Wearables, Fitness-Apps und der Datenschutz: Welche Bedenken haben Verbraucher? Und wie schätzen sie mögliche Folgen der Nutzung ein?

Datenschutzbedenken aller Befragten



Quelle: „Wearables, Fitness-Apps und der Datenschutz“ – Eine Untersuchung der Verbraucherzentralen im Rahmen des Projektes Marktwächter Digitale Welt.

Methodik: Ergebnisse auf Basis einer repräsentativen Telefonbefragung mit 1055 Personen ab 14 Jahren, die in den letzten drei Monaten das Internet genutzt haben.

Erhebungszeitraum: 25.08 - 29.09. 2016

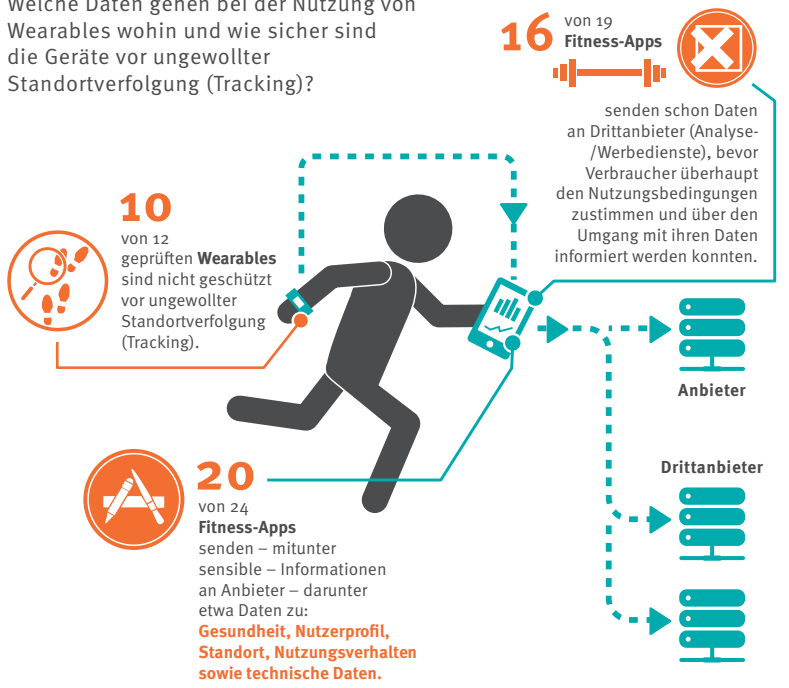
Durchführendes Institut: mindline media GmbH

Fehlertoleranz der Gesamtstichprobe: max. +/- 3 Prozentpunkte (bei einem Anteilswert von 50 Prozent).

DATEN AUßER KONTROLLE: FITNESS-APPS SENDEN ZAHLREICHE VERBRAUCHERDATEN



Welche Daten gehen bei der Nutzung von Wearables wohin und wie sicher sind die Geräte vor ungewollter Standortverfolgung (Tracking)?



Quelle: „Wearables, Fitness-Apps und der Datenschutz“ – Eine Untersuchung der Verbraucherzentralen im Rahmen des Projektes Marktwächter Digitale Welt.

Methodik: Untersucht wurden zwölf Wearables und die jeweiligen verfügbaren Fitness-Apps für die Betriebssysteme iOS und Android.

Erhebungszeitraum: 01.07. - 11.08.2016

Durchführendes Institut: datenschutz nord GmbH.

Gefördert durch:



aufgrund eines Beschlusses des Deutschen Bundestages

Stand: April 2017

verbraucherzentrale

IMPRESSUM:
Verbraucherzentrale NRW e.V.
Mintropstr. 27
40215 Düsseldorf

Die Untersuchung „Wearables, Fitness-Apps und der Datenschutz“ wurde im Rahmen des Projektes Marktwächter Digitale Welt durchgeführt.