



Ansbach, den 5. Dezember 2016

## Pressemitteilung

### Datenschutzaufsichtsbehörden prüften Wearables

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) beteiligte sich an einer deutschlandweiten Prüfkaktion und prüfte gemeinsam mit sechs weiteren Aufsichtsbehörden Wearables. Auf dem Prüfstand standen sowohl Fitness-Armbänder als auch Smart Watches mit Gesundheitsfunktionen. Außerdem wurden die Apps der Hersteller einer technischen Analyse unterzogen. Das Ergebnis war eindeutig: kein Gerät erfüllt vollständig die datenschutzrechtlichen Anforderungen.

Wearables, auch bekannt unter dem Begriff Fitness-Armbänder oder Activity-Tracker, sollen den Nutzer zu einer gesunden Lebensweise motivieren und die Bewegung im Alltag fördern. Schon lange können die Geräte Schritte zählen, zurückgelegte Kilometer messen und verbrauchte Kalorien erfassen. Doch die aktuellsten Wearables bieten noch viel mehr. Die geprüften Geräte überwachen die Herzfrequenz, bestimmen die Körpertemperatur über Sensoren auf der Haut und geben Rückmeldung über den Schlafrythmus. Diese Angaben interessieren immer mehr Versicherer und Unternehmen der Gesundheitsbranche, sodass es sich lohnt, die Geräte genauer unter die Lupe zu nehmen.

Das BayLDA überprüfte zusammen mit den Datenschutzaufsichtsbehörden aus Schleswig-Holstein, Brandenburg, Niedersachsen, Nordrhein-Westfalen und Hessen sowie der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit insgesamt 16 Wearables von Herstellern, die ca. 70% des Marktanteils in Deutschland abdecken.

Geprüft wurden zum einen rechtliche Fragestellungen, wie z. B. die ausreichende Aufklärung über den Datenumgang oder die Frage, ob tatsächlich Gesundheitsdaten verarbeitet werden. Auch die Technik stand im Fokus. In drei deutschen Prüfzentren wurden die Geräte sowie deren Hersteller-Apps für die Betriebssysteme iOS und Android im Labor getestet. Es wurden die Datenflüsse analysiert, um festzustellen, wer auf welche Daten Zugriff bekommen kann. Außerdem war ein Blick auf die Apps notwendig. Ohne die dazugehörigen Apps sind die meisten Wearables in ihrer Funktion erheblich eingeschränkt oder sogar unbrauchbar. Diese getesteten Apps wurden durch die Nutzer zusammen mehr als 30 Mio. Mal heruntergeladen.

Die Ergebnisse der Prüfung zeigen zahlreiche Mängel auf:

- **Transparenz? Nachvollziehbarkeit? Fehlanzeige!**

Wer Wearables nutzt, muss zur Kenntnis nehmen, dass oftmals zahlreichen Firmen die Daten erhalten. Hersteller und Betreiber geben sich keine Mühe, Licht in das Dickicht aus Hardware-Hersteller, App-Betreiber, App-Shop-Anbieter und zahlreichen Dienstleistern zu bringen. Für den Nutzer bedeutet das, dass er sich oftmals nur pauschalen Datenschutzerklärungen gegenüber sieht und keine Chance hat, zu erkennen, wer für was zuständig ist und was mit den eigenen Daten bei wem passiert. Tests, bei den

Anbietern Auskunft über die gespeicherten Daten zu erhalten, wurden entweder mit pauschalen Verweisen auf Datenschutzerklärungen beantwortet oder wegen vermeintlicher Nicht-Zuständigkeit abgewiesen. Hinzu kommt, dass die Anbieter teilweise im Ausland sitzen und nur eine internationale E-Mail-Adresse als Kontaktmöglichkeit anbieten.

- **Besonders schützenswerte Daten**

Die Aufgabe der Fitness-Tracker und Apps ist es, Gesundheitsdaten und damit besonders schützenswerte Daten der Nutzer zu verarbeiten. Zwar sind die Einzelinformationen wie z. B. Körpergewicht, zurückgelegte Schritte, Dauer des Schlafes oder Herzfrequenz für sich betrachtet oftmals wenig aussagekräftig. In der Regel werden diese Daten jedoch mit eindeutig zugewiesenen Personenkennungen verbunden. Bei einer dauerhaften Nutzung fallen derart viele Informationen an, dass sich daraus ein erstaunlich präzises Bild des Tagesablaufs und Gesundheitszustands des Nutzers ergibt (was der Nutzer des Gerätes auch bezweckt). Insbesondere bei Verknüpfung der Einzelinformationen mit Standortdaten ergibt das sehr persönliche Informationen:

- Wann bin ich morgens aufgestanden?
- Habe ich unruhig geschlafen, (da ich am Vorabend Alkohol konsumiert habe)?
- Wo beginnt und endet mein Weg zur Arbeit?
- Warum bin ich aufgereggt und wieso schlägt mein Herz höher, obwohl ich seit 30 min auf dem Bürostuhl sitze?
- ...

All diese Fragen lassen sich beantworten, wenn die Daten der Wearables ausgewertet werden. Kritisch wird dieses insbesondere dadurch, dass viele der Geräte die Daten extern durch Dritte verarbeiten lassen und durch die unklaren Regelungen der Nutzer keine Kontrolle mehr darüber hat, wer die Daten von ihm sonst noch hat.

- **Datenschutzbestimmungen**

Datenschutzbestimmungen sollen den Nutzer in die Lage versetzen, zu erkennen, wer welche Daten von ihm zu welchen Zwecken erhebt, was er damit macht und insbesondere auch, an wen er welche Daten weitergibt bzw. wer sonst noch Zugriff darauf hat. Die meisten Datenschutzerklärungen erfüllten diese gesetzlichen Anforderungen nicht. Sie waren in der Regel viele Seiten lang, schwer verständlich, enthielten zu essentiellen Datenschutzfragen nur pauschale Hinweise und waren teilweise nicht einmal in deutscher Sprache vorhanden. So erfährt der Nutzer oftmals nicht im ausreichenden Maße, wer konkret Zugriff auf die Daten hat und wie lange sie gespeichert werden. Dabei wäre es ein Leichtes, dies in wenigen kurzen Sätzen zu beschreiben. Oftmals wurde auch nur auf die generelle Datenschutzerklärung des Unternehmens verwiesen, die kaum konkreten Bezug zu dem Wearable hat.

Erstaunlich ist auch, dass fast kein Gerätehersteller über die besonders schützenswerten Gesundheits- und Standortdaten aufklärt - ganz im Gegenteil: einige Hersteller waren sogar der Auffassung, dass es sich dabei um anonyme Daten handle.

- **Daten mit Freunden teilen**

Viele Geräte und Apps bieten die Möglichkeit, die aufgezeichneten Fitness-Daten mit Freunden z. B. über soziale Netzwerke zu teilen. Die Funktion soll den Nutzer zu häufigem Training und Bestleistungen anspornen und das gemeinsame Training fördern. Da hierbei auch sehr sensible Informationen preisgegeben werden können, darf das jedoch nur dann geschehen, wenn der Nutzer es ausdrücklich wünscht.

- **Datenweitergabe an Dritte**

Beunruhigend sind auch die Aussagen vieler Hersteller zur Datenweitergabe. Einige Hersteller stellen klar, dass sie die Fitness-Daten der Nutzer für eigene Forschungszwecke und Marketing verwenden und an verbundene Unternehmen weitergeben. Der Nutzer erfährt weder, um wen es sich dabei handelt, noch kann er widersprechen. Ein klarer Verstoß gegen deutsches Datenschutzrecht.

- **Reichweitenmessung**

Die technische Analyse brachte mehr Licht ins Dunkel. Fast alle Hersteller setzen Tracking-Tools US-amerikanischer Unternehmen ein. Mithilfe dieser Tools können Hersteller erfassen, wie die Geräte oder Apps genutzt werden, um die Benutzerfreundlichkeit zu verbessern. Die Daten können aber auch für Werbezwecke und zur Profilbildung verwendet werden. Zwar wird oft angegeben, dass hierzu nur anonyme Daten verwendet werden würden. Den Nachweis bleiben die Hersteller jedoch schuldig. Die Erfahrung zeigt, dass in der Regel in solchen Fällen weiterhin bei vielen Daten ein Personenbezug hergestellt werden kann.

- **Datenlöschung**

Die Geräte sind schnell verloren oder technisch überholt, sodass zahlreiche Nutzer ihre gebrauchten Geräte weiterverkaufen wollen. Das birgt ein enormes Risiko. Nutzer glauben, dass mit dem Löschen der App alle Daten vernichtet sind. Das ist falsch! Bei vielen Geräten hat der Nutzer keine Möglichkeit, seine Daten selbstständig vollständig zu löschen. Weder im Gerät selbst noch im Nutzerkonto gibt es eine Löschfunktion. Einige Hersteller weisen sogar darauf hin, dass eine Löschung nicht möglich ist. Wie lange die Hersteller die Daten speichern, bleibt verborgen. Fakt ist, dass es sich hierbei um einen gravierenden Verstoß handelt.

*„Aufgrund unserer zahlreichen Prüfungen der letzten Jahre im Bereich Internet und smarte Geräte haben wir viel Erfahrung gesammelt. Auch diese Prüfung offenbarte Mängel im Datenschutz, die wir bereits bei anderen Testgeräten feststellten. Dass die Unternehmen ihren Aufklärungspflichten nicht immer vollständig nachkommen, ist bekannt. Mit Erschrecken mussten wir feststellen, dass gerade in sensiblen Bereichen wie Gesundheit und Bewegungsprofile die Daten häufig an Dritte übermittelt werden. Der Nutzer ist aufgrund der mangelnden Transparenz nicht mehr Herr seiner Daten und hat keine Chance zu verfolgen, in wessen Hände seine Gesundheitsdaten gelangen“,* erklärte Thomas Kranig, der Präsident des BayLDA.

Einige Mängel ließen sich problemlos dadurch beheben, dass die Fitnessdaten der Wearables lediglich auf das Smartphone weitergeleitet und lokal verarbeitet werden. Eine permanente Übermittlung aller Daten vom Smartphone an Server diverser Firmen ist aus Sicht der Datenschützer in der Regel mit Risiken verbunden, denen sich die Nutzer bewusst sein sollten.

*„Würden die Hersteller dieser Empfehlung nachkommen, würden in den wenigsten Fällen Gesundheitsdaten in die Hände Dritter gelangen. Die heutigen Smartphones sind so leistungsstark, dass sich dies ohne Funktionseinschränkung technisch ganz einfach umsetzen ließe. Indem die Hersteller jedoch alle Daten von der App weiterleiten, signalisieren sie ein eigenes Interesse an den sensiblen Daten. Das macht uns misstrauisch“,* so Thomas Kranig, der Präsident des BayLDA.

Im April 2016 hatte sich die Konferenz der unabhängigen Datenschutzbehörden mit einer EntschlieÙung<sup>1</sup> an die Hersteller von Wearables und Gesundheits-Apps gewandt und Datensparsamkeit, Transparenz, korrekte

---

<sup>1</sup> [http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/91DSK\\_EntschliessungWearables.html?nn=5217228](http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/91DSK_EntschliessungWearables.html?nn=5217228)

Einwilligungserklärungen und Verantwortungsübernahme eingefordert. Die aktuellen Prüfungsergebnisse unterstreichen noch einmal die Dringlichkeit dieser Forderungen.

Im Rahmen der Zuständigkeit werden die an der Prüfung beteiligten Datenschutzaufsichtsbehörden nun an die Hersteller herantreten und zu erreichen suchen, dass sie die o.g. Mängel abstellen.

Thomas Kranig  
Präsident