Clemens Putschli

Wearables und Datenschutz

Datenschutz bei der Entwicklung des PARADISE Wearables

Laptops, Tablets und Smartphone sind längst nicht mehr die einzigen tragbaren Computer. Sogenannte Wearables, wie beispielsweise Armbanduhren oder Brillen, speichern unzählige persönliche Daten ihrer Nutzer und verhalten sich häufig nicht datenschutzkonform. Im Rahmen des PARADISE Projektes wurde daher ein datenschutzkonformes Wearable entwickelt

1 Was sind Wearables?

Unter dem Begriff der Wearable Computing Devices (im folgenden Wearables) werden elektronische Geräte verstanden, welche während ihrer Nutzung am oder in unmittelbarer Nähe zum Körper getragen werden. Ein Wearable ist dabei als tragbarer, anziehbarer oder sogar kleidsamer Computer zu verstehen. Hörgeräte und Herzschrittmacher können daher beispielsweise als erste simple Wearables bezeichnet werden. Heutige Wearables beinhalten normalerweise einen oder mehrere Sensoren und verfügen über eine digitale Schnittstelle (beispielsweise Bluetooth oder WLAN) nach außen. Über diese Schnittstelle werden die Sensordaten auf ein Smartphone oder direkt auf einen Server im Internet übertragen. Aufgrund dieser Schnittstelle sind Wearables auch als Teil des „Internet der Dinge" zu sehen.[1] In den meisten Wearables sind eine Vielzahl von unterschiedlichen Sensoren eingebaut. Dies kann vom simplen Beschleunigungssensor, als Schrittzähler, über einen GPS Chip, zur Positionsbestimmung, bis hin zu kombinierten Sensoren, welche beispielsweise Herzfrequenz und Körpertemperatur erfassen, gehen. Wearables werden jedoch nicht nur direkt am Körper getragen, sondern können auch Teil der Kleidung sein. So wird das Wearable zum Alltagsbegleiter. Die dabei erfassten Sensordaten geben meist tiefe Einblicke in das Privatleben der Nutzer und unterliegen deshalb besonders hohen Datenschutzanforderungen.

Der Begriff Wearable wird im Allgemeinen als Sammelkategorie für unterschiedliche Anwendungsformen verstanden, kategorisiert durch den Ort, wo das Gerät am Körper getragen wird:

- Wristwear (Smart Watches und Fitness Armbänder);
- Eyewear (Datenbrillen und smarte Kontaktlinsen);
- Earwear (smarte Kopfhörer);
- Smarte Kleidung.[2]

2 Datenschutz und Wearables

Es ist zu beobachten, dass Wearables häufig zum Zweck der Selbstüberwachung und Selbstvermessung von körperlicher und sportlicher Aktivität genutzt werden. Gerade die Digitalisierung erleichtert dabei die Integration in den Alltag des Trägers. Wearables können passende Daten automatisiert aufzeichnen und später dem Nutzer wiederspiegeln. Obwohl noch nicht endgültig geklärt ist, ob Wearables den Träger zu einem gesunderen Lebensstiel motivieren, werden sie beispielsweise als Dienstleistung der Krankenkassen angeboten.[3] Zwar ist es gesetzlichen Krankenkassen grundsätzlich verboten personenbezogene Daten ihrer Mitglieder zu erheben, welche über das für die Vertragserfüllung erforderliche Maß hinausgehen, dennoch werden Wearables und auch Fitness Apps zurzeit schon freiwillig als automatisiertes Bonusheft eingesetzt.[4] Eine solche Nutzung wirft die Frage auf, inwiefern die Verwendung eines Wearables langfristig eine wirklich freiwillige Entscheidung bleibt. Diese Fragestellung gilt natürlich nicht nur für Krankenkassen, sondern gerade auch für alle anderen Konstellationen, welche durch ein besonderes Machtgefälle gekennzeichnet sind. Hierzu zählt beispielsweise der gezielte Einsatz von Wearables in Betrieben, aber auch der Einsatz von Wearables bei Dopingkontrollen von Spitzensportlern.

3 Datenschutz durch ein Wearable

Es stellt sich daher die Frage, inwieweit ein Wearable so gestaltet werden kann, dass dessen Einsatz bei der Dopingkontrolle daten-

1 Vgl. *Roßnagel/Jandt/Skistims/Zirfas*, Datenschutz bei Wearable Computing: Eine juristische Analyse am Beispiel von Schutzanzügen, Springer-Verlag, 2012.

Clemens Putschli

Wissenschaftlicher Mitarbeiter am Fraunhofer-Institut für Angewandte Informationstechnik FIT in Sankt Augustin, Projekt PARADISE.

E-Mail:
clemens.putschli@fit.fraunhofer.de

2 Dazu insgesamt *Herrmann*, Wearables Chancen und Risiken, Universität Siegen 2016, Online verfügbar unter http://dhgo.to/wearable-privacy (letzter Abruf 23.10.2017).

3 Die AOK Nordost bietet beispielsweise seit Januar 2016 die App „FitMit AOK" an. Online verfügbar unter https://www.fitmit-aok.de/ (letzter Abruf 24.10.2017).

4 *Moll/Schulze/Rusch-Rodosthenous/Kunke/Scheibel*, Wearables, Fitness-Apps und der Datenschutz: Alles unter Kontrolle?. Verbraucherzentrale NRW e.V. (Hrsg.) 2017. Online verfügbar unter: http://www.marktwaechter.de/sites/default/files/downloads/mw-untersuchung_wearables_0.pdf (letzte Abruf 23.10.2017).

schutzkonform ist.[5] Zurzeit betreibt die Welt-Anti-Doping-Agentur (WADA) ein Online-Meldesystem bei dem Spitzensportler ihre zukünftigen Aufenthaltsorte für 3 Monate im Voraus hinterlegen müssen. Diese Daten werden genutzt um unangekündigte Dopingkontrollen bei den Athleten durchzuführen. Die Dopingkontrollen müssen für den Sportler unvorhersehbar sein, damit die Chance auf eine Verschleierung von Dopingverstößen reduziert wird.

Um ein nachvollziehbares Verfahren zur Planung und Durchführung von Dopingkontrollen zu erhalten, entwickelte das PARADISE Projekt ein System, welches einerseits unangekündigte Kontrollen ermöglicht und andererseits die Privatsphäre der Athleten schützt. Die dazu entwickelte datenschutzkonforme Lösung nutzt ein sogenanntes „EVES-Device", um den Athleten unvorhersehbar zu lokalisieren. Hierbei handelt es sich um ein Wearable, welches eine Positionsbestimmung des Sportlers per Fernabfrage ermöglicht. Obwohl dies auf den ersten Blick hin wie eine erhöhte Datenaufnahme aussieht, dient es der Reduzierung der Datenaufnahme beim Dopingkontrollprozess. Durch die dahinterstehende PARADISE-Plattform und dem dazugehörenden EVES-Device muss eine genaue Positionierung nur unmittelbar vor einer unangekündigten Dopingkontrolle abgefragt werden. Das PARADISE-System wurde datenschutzrechtlich nach dem Standard-Datenschutzmodell (SDM) beurteilt. Hierbei wurde deutlich, dass die Plattform unter Einbindung des EVES-Device dem hohen Schutzstandard der Sportlerdaten gerecht wird. Es ist hierbei natürlich zu beachten, dass ein unvorhergesehenes Dopingkontrollsystem immer eine Abwägung der Grundrechte auf informelle Selbstbestimmung mit der Datenerhebung für Dopingkontrollen darstellt. Die Sportler dürfen beispielswiese nicht im Vorfeld über die anstehende Kontrolle informiert werden und müssen Angaben zu ihren Gesundheitsstatus machen.[6]

4 Datenschutz bei der Entwicklung des PARADISE Wearables

Für die Entwicklung eines datenschutzkonformen Wearables wurden unter anderem die drei essentiellen Datenschutztechniken Datenminimierung, Transportverschlüsselung und Vertraulichkeit der Daten beachtet.[7]

4.1 Datenminimierung:

Das Wearable darf nur genauso viele Daten wie nötig aufnehmen. Die aufgenommenen personenbezogenen Daten müssen auf das für den Zweck der Verarbeitung erforderliche Maß beschränkt sein. Aus diesem Grund werden bei dem EVES-Device beispielsweise nicht dauerhaft die Positionsdaten aufgezeichnet. Nur wenn eine Positionsabfrage von außen getriggert wird, werden diese Daten abgefragt, aufbereitet, an den PARADSIE-Server gesendet und danach vom Gerät gelöscht.

4.2 Transportverschlüsselung:

Damit keine externe Partei Zugriff auf die Daten des Wearable bekommen, müssen Anfragen und Antworten des Wearables verschlüsselt werden. Hierzu kann beispielsweise eine verschlüsselte Datenverbindung (TLS 1.2) genutzt werden. Das EVES-Devices verwendet als Datenkanal jedoch SMS, um auch bei schlechten Mobilfunkempfang eine Datenverbindung zu ermöglichen und um einen weltweiten Einsatz zu gestatten. Da eine SMS grundsätzlich nicht verschlüsselt versendet wird, verschlüsselt das EVES-Device alle Kommunikation über diesen Kanal mit einem symmetrischen Schlüssel. Hierzu wurde eine AES-256 Verschlüsselung gewählt. Die übermittelten Daten sind somit für Unbefugte nicht lesbar.

4.3 Vertraulichkeit der Daten:

Die Daten, welche durch ein Wearable aufgenommen wurden, dürfen nur an die dazu ermächtigte Instanz weitergegeben werden. Es muss darauf geachtet werden, dass die erhobenen Daten nicht von anderen Geräten gelesen und genutzt werden. Gerade Positionsdaten sind für eine Profilbildung des Nutzes bedeutungsvoll. Dabei ist auch zu beachten, dass ungewollt eine Profilbildung über unscheinbare Metadaten möglich ist. Dies kann beispielsweise bei einer Datenauswertung auf einem fremden Server geschehen. Im PARADISE-Projekt ist die dahinterstehende Serverinfrastruktur durch die Sealed-Cloud Technologie abgesichert.[8] Zusätzlich werden alle genutzten Server auf vertrauenswürdiger Infrastruktur gehosted. Gleichzeitig ist das EVES-Devices so konzipiert, dass es nur mit einem passenden Schlüssel abgefragt werden kann. Die möglichen Kommunikationskanäle des EVES-Device wurden extra auf ein Minimum reduziert. So ist es beispielsweise nicht möglich die Positionsdaten über Bluetooth oder WLAN zu erhalten.

4.4 Der Weg zum Wearable

Im Rahmen des PARADISE-Projektes wurden unterschiedliche Iterationen durchlaufen um ein datenschutzkonformes Wearable zu erstellen. Die grundsätzliche Idee dazu war es, eine aus der Sicht des Sportlers autarke Blackbox zu schaffen. Der Sportler sollte es bei sich tragen, aber eine Interaktion mit dem Gerät war nicht vorgesehen. Die erste Version des Eves-Devices konnte beispielsweise nicht einmal deaktiviert werden. Um eine einfache Handhabe zu gewährleisten, kann das Gerät über eine QI-Ladeschnittstelle drahtlos aufgeladen werden. Im Laufe der Entwicklung ist das EVES-Device aber auch um eine Ladestandsanzeige und eine Möglichkeit zum Deaktivieren des kompletten Gerätes erweitert worden. Parallel dazu wurden unterschiedliche Gehäuseprototypen entwickelt und getestet. Das EVES-Device ist dabei immer in die beiden Wearable Kategorien „Wristwear" und „Smarte Kleidung" einzuordnen. Im Rahmen des Projektes wurde mit verschiedenen Konzepten experimentiert. Die Abbildung 1 zeigt die unterschiedlichen Prototypen.

5 Das PARADISE Forschungsprojekt hat sich zur Aufgabe gesetzt, ein derartig datenschutzkonformes Wearable zu entwickeln.

6 *Herber/Jentsch/Zickau*, Datenschutz und Dopingkontrollen, DuD 2017, S. 427-433.

7 *Roßnagel*, Datenschutz in einem informatisierten Alltag, Stabsabteilung der Friedrich-Ebert-Stiftung (Hrsg.) 2007, S. 158-174.

8 *Jaeger/Monitzer/Rieken/Ernst/Nguyen*, Sealed Cloud – A Novel Approach to Safeguard against Insider Attacks, in: Krcmar/Reussner/Rumpe, Trusted Cloud Computing 2014, pp 15-34.

Abbildung 1 | Unterschiedliche EVES-Device Prototypen

Während der Entwicklung fiel auf, dass vor allem die Lokalisierung viele datenschutzrechtliche Probleme mitbringt. Eine Lokalisierung, welche nur über ein GNSS System erfolgt, wie beispielsweise GPS, ist datenschutzrechtlich problemlos möglich. Denn für diese Positionierung werden keine Daten bei einem fremden Server ausgewertet[9]. Sobald jedoch die reine GNSS Positionierung nicht möglich ist, wird ein zusätzlicher Dienst benötigt. Gerade in Gebäuden ist keine genaue GNSS Positionierung verfügbar.

Um die Positionierung ausfallsicherer zu gestalten nutzt das entwickelte EVES-Device beispielsweise zusätzlich das GSM Netz. Dabei wird die zurzeit genutzte Cell-ID des Mobilfunkbetreibers ermittelt und über einen Server in eine Positionskoordinate umgewandelt. Diese Umwandlung wird von verschiedenen Dienstanbietern angeboten, wie z. B. Google oder Mozilla. Durch einen externen Dienstanbieter wäre der Datenschutzrechtliche Grundsatz der Vertraulichkeit jedoch nicht mehr gegeben[10]. Aus diesem Grund wird die dazu benötigte Datenbank auf einem Server des PARADISE Projektes implementiert.

Die über die Cell-ID ermittelte Position ist jedoch recht ungenau. Es treten in städtischen Gebieten in der Regel Ungenauigkeiten von ca. 100 – 200 m auf, in ländlichen Gebieten können aber auch zu Ungenauigkeiten von bis zu mehreren Kilometer möglich sein.

Um die Ungenauigkeit der Cell-ID Lokalisierung zu verbessern, könnte als Ergänzung eine Lokalisierung über WLAN implementiert werden. Dabei werden die Adressen der umliegenden WLAN Netze gescannt und ebenfalls über einen Server abgeglichen. Für eine genaue Lokalisierung müsste die Anzahl der hinterlegten WLAN Netze äußerst groß sein. Als problematisch könnte sich ferner die Aktualität der WLAN Netze herausstellen, da private Netze in einem ständigen Wandel sind und demnach nicht als einzige verlässliche Lokalisierungsquelle angesehen werden können. Öffentliche Einrichtungen, wie Museen oder Cafés, die länger bestehen, können zusätzlich als Bezugsquelle genutzt werden, da diese meist mehrere Jahre über den gleichen Standort mit der gleichen WLAN Adresse verfügen. Die dafür benötigte Datenbank wäre aber folglich in einem ständigen Wandel. Um die Daten aktuell zu halten, müsste auf andere Anbieter solcher Datenbanken zurückgegriffen werden, wie beispielsweise Google oder Mozilla. Dieser Rückgriff würde aber mit zusätzlichen neuen datenschutzrechtlichen Probleme einhergehen[11].

5 Warum Apps nicht das richtige Werkzeug sind

Auf den ersten Blick wirkt es, als wenn die Funktionen des EVES-Device auch durch eine Smartphone App abgedeckt werden können. Ein wichtiger Vorteil wäre, dass bei einer Software Lösung keine dezidierte Hardware benötigt wird. Der zusätzliche Aufwand für Hardwareenwicklung und Produktdesign würde wegfallen und auch das Deployment einer App scheint einfach über den Smartphone AppStore zu funktionieren. Selbst zukünftige Updates könnten bei einer App sehr viel einfacher ausgerollt werden.

Das größte Problem besteht bei einer App jedoch in den unkontrollierbaren Zugriffsmöglichkeiten auf die Daten. Im PARADISE-System ist es von zentraler Bedeutung, dass keine Informationen über eine mögliche Dopingkontrolle vorab an den Nutzer weitergegeben werden. Dopingkontrollen müssen unvorhersehbar durchgeführt werden. Durch die vor einer Dopingkontrolle stattfindende Ortungsfunktion, könnte das EVES-Device aber als Kontrollvorwarngerät verwendet werden.

Damit der Sportler nicht vorgewarnt ist, müssten regelmäßig wiederkehrende unwirksame Positionsabfragen (sogenannte Fake-Abfragen) an das EVES-Device gesendet werden. Um eine dauerhafte Überwachung des Sportlers zu unterbinden, werden bei Fake-Anfragen keine echten Positionsangaben an das PARADISE- System gesendet. Bei einer Smartphone-App könnte jedoch von außen sehr leicht überprüft werden, ob die Ortungsfunktion genutzt wurde. Könnte der Sportler Fake-Anfragen von echten Anfragen jedoch auf diese Weise unterscheiden und wäre vor einer unangekündigten Dopingkontrolle gewarnt.

Ein Wearable kann mit sehr einfachen Mitteln vor Zugriff von außen abgesichert werden. Beispielswiese kann das Wearable abgeschirmt und gleichzeitig komplett eingeschweißt und versiegelt werden. Bei einer Dopingkontrolle muss das Wearable nur auf seine Unversehrtheit überprüft werden. Diese Überprüfung könnte aber vor Ort von einem Doping-Kontrolleur durchgeführt werden.

6 Fazit

Die Ausführungen zeigen, die Entwicklung eines datenschutzkonformen Wearables ist auch im Anti-Doping Bereich möglich. Obwohl ein Wearable als ständiger Begleiter den kompletten Kontext des Benutzers erfassen kann, kann es auch so entwickelt werden, dass es datenschutzkonform eingesetzt werden kann. Hierzu müssen jedoch die erhobenen Daten geringgehalten und die Kommunikation verschlüsselt werden. Weiterhin ist es wichtig, dass die aufgenommenen Daten vertraulich behandelt werden und keine Profilbildung von außen ermöglicht wird.

9 Vgl. *LaMance/DeSalas/Järvinen*, Innovation: Assisted GPS: A Low-Infrastructure Approach, GPS World, 2002. Online verfügbar unter: http://gpsworld.com/innovation-assisted-gps-a-low-infrastructure-approach (letzter Abruf 24.10.2017).

10 Das Standard-Datenschutzmodell Version 1.0, https://datenschutzzentrum.de/uploads/SDM-Methode_V_1_0.pdf (letzter Abruf: 24.10.2017), S. 13.

11 Dazu *Li/Sun/Zhu/Lu/Cheng*, Achieving privacy preservation in WiFi fingerprint-based localization, IEEE Conference on Computer Communications, Toronto, 2014, S.2337-2345.