



Protokolliertes Leben

Datenschutzrechtliche und sicherheitstechnische
Risiken und Nebenwirkungen von
Fitness-Trackern

Über das AV-TEST Institut

- Mehr als 35 IT-Spezialisten
- Mehr als 15 Jahre Expertise im Bereich Antivirenforschung
- Unternehmensgründung 2004
- Eine der weltweit größten Virendatenbanken
- 500 Client- und Server-Systeme
- Mehr als 2.500 Terabyte Testdaten
- Mehr als 5.000 Einzel- und Vergleichstests pro Jahr
- Analyse, Testing, Development, Consulting & Services für Hersteller, Fachmagazine, Behörden & Unternehmen



AGENDA



Wer

... hat Interesse an den Daten?

Warum

... haben sie Interesse?

... sollte uns das interessieren?

Wie

... erlangen sie Zugriff auf die Daten?



Wer hat Interesse an den Daten?

(Cyber) Kriminelle



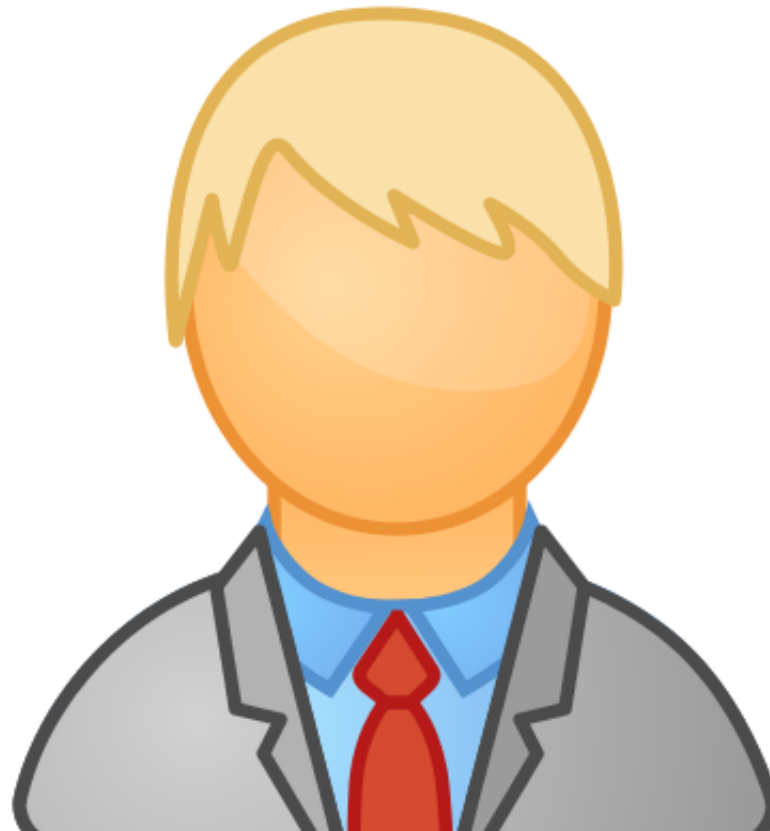
Wer hat Interesse an den Daten?

User



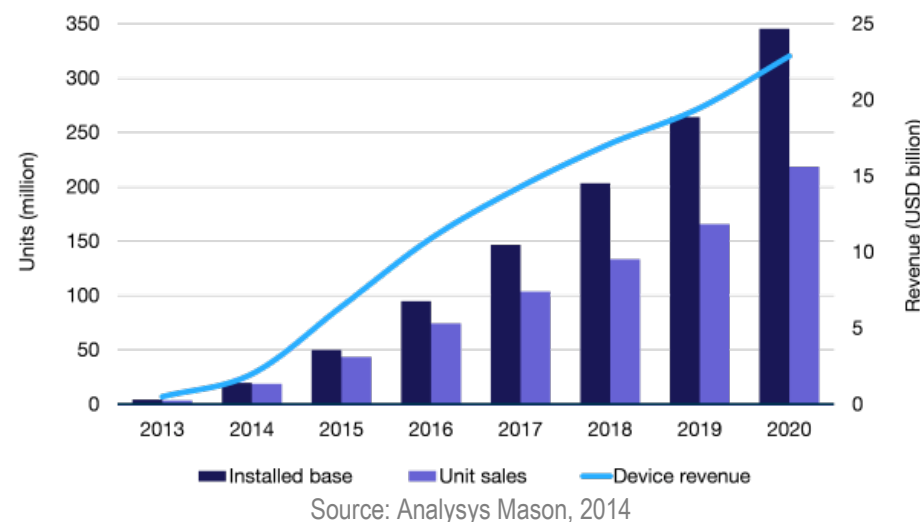
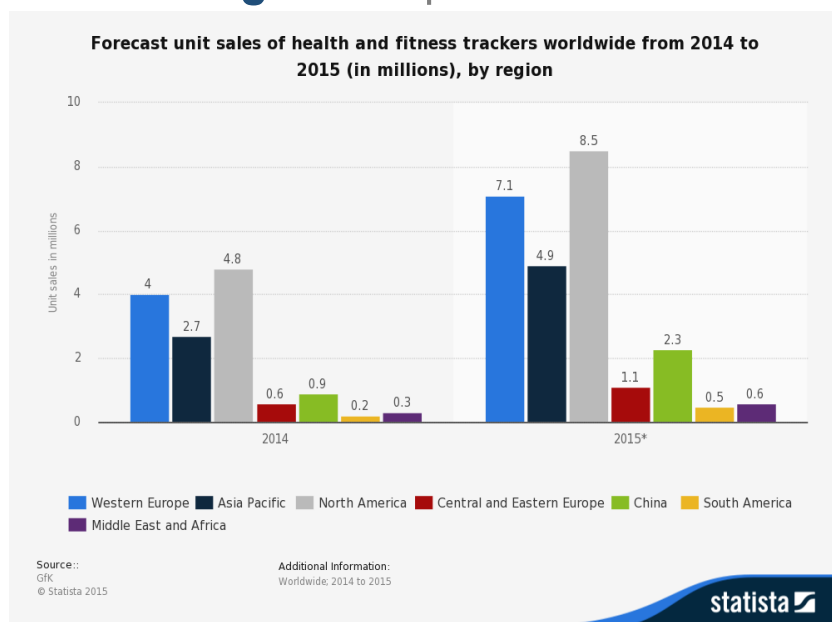
Wer hat Interesse an den Daten?

Konzerne / Behörden



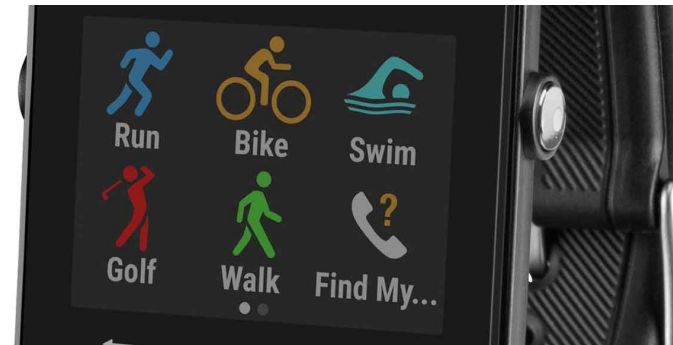
Warum haben sie Interesse an den Daten?

- Fitness Tracker könnten **das nächste „große Ding“** sein mit **Millionen von Nutzern**
- Keine oder **keine nennenswerten Sicherheitskonzepte**
- **Unmengen** von potentiell interessanten und **sensiblen Daten** werden erfasst



Warum haben sie Interesse an den Daten?

- Welche Arten von **Rohdaten** werden erfasst?
 - Accelerometer
 - Pedometer
 - Pulsmessung
 - Blutsauerstoff
 - GPS
 - UV Belastung
 - Umgebungslichtmessung
 - Hauttemperatur
 - Hautwiderstandsmessung
 - Alle möglichen Notifizierungen vom Smartphone (SMS, eMail, WhatsApp,... App Permissions!)
- **Datenarten einzeln betrachtet** erscheinen auf den ersten Blick **nicht als sensibel...**



Warum haben sie Interesse an den Daten?

- Was für **Daten** lassen sich daraus **ableiten**?
 - Noch Intuitiv
 - Stress-Level
 - Gemütslage
 - Schlafqualität
 - Aktivitätenarten und –Level (Walking, Running, Biking, Driving – Indoor / Outdoor)
 - Zurückgelegte Distanzen / Besuchte Orte
 - ...nicht mehr ganz so intuitiv
 - Raucher / Nicht-Raucher
 - Zeitpunkt und Intensität Alkoholkonsum
 - Schwangerschaft
 - Zwischenmenschliche Verbindungen (Hierarchie, Sympathie/Antipathie)
 - ...usw. usw. → **Data Mining und Machine Learning** kennen hierbei kaum Grenzen, **mit genügend Daten sind überraschende Assoziationen möglich!**

Your Activity Tracker Knows When You Quit Smoking

**Working-Relationship Detection
from Fitbit Sensor Data**

Warum haben sie Interesse an den Daten?

- Personal Data ist jede Menge Geld wert!

Company name	Facebook	LinkedIn	Yahoo	Google
Market cap (in billions)	\$100.56	\$31.31	\$27.67	\$282.20
Number of users (in millions)	1,110	225	627	1,300
Revenue (in billions)	\$1.813	\$0.366	\$1.135	\$13.110
Per user valuation	\$90.59	\$131.55	\$44.13	\$217.08
Average Revenue per User (ARPU)	\$1.63	\$1.53	\$1.81	\$10.09



YAHOO!

LinkedIn

Warum haben sie Interesse an den Daten?

- **Versicherungsunternehmen** bieten **Boni** und **spezielle Tarife**
 - Vitality (UK): „The healthier you get, the more we're able to offer you. It's a virtuous circle that's good for you, good for us, and good for society.“
- **Deutsche Versicherungsunternehmen:**
 - „Nach der AOK Nordost hat inzwischen auch die Techniker Krankenkasse Wearables und Fitnesstracker offiziell in ihr Bonusprogramm aufgenommen – darunter auch die Apple Watch.“ <http://heise.de/-2817046>
 - Behaupten **allerdings** sie sind (noch) **nicht an den Daten** selbst **interessiert**
- **Arbeitgeber** erkennen den Nutzen

Tracking im Job

Schläfst du noch, oder arbeitest du schon?

Die Wearable-Technologie ist ein riesiger Wachstumsmarkt. Was als Werkzeug für freiwillige Selbstoptimierer begann, könnte zum Instrument der Kontrolle werden.

- Beim **Nutzer** steigt Motivation zur Manipulation (echter **monetärer Nutzen**)
- **Angreifer** erhalten **neues Druckmittel** mit Androhung auf **Löschung oder Manipulation** der Nutzerdaten

Warum haben sie Interesse an den Daten?

- **Tracking** des Nutzers wird weiter **vereinfacht**
 - “Security Expert Warns of Criminals Using Facebook to Plan Home Burglaries”
 - Der **Standort des Nutzers** kann nun direkt vom Gerät des Nutzers gelesen werden
 - „**Gesundheits-Schufa**“ verhindert, dass man die Versicherung, den Kredit oder den Job bekommt, den man sich wünscht
- “**Wearable tech** will transform sport – but will it also **ruin athletes' personal lives?**”
 - Mit manipulierten, erzeugten oder gelöschten Daten können Karrieren gestützt oder zerstört werden
- Verwendung als **legitime Beweismittel vor Gericht**

Fitbit Data to Be Submitted as Court Evidence

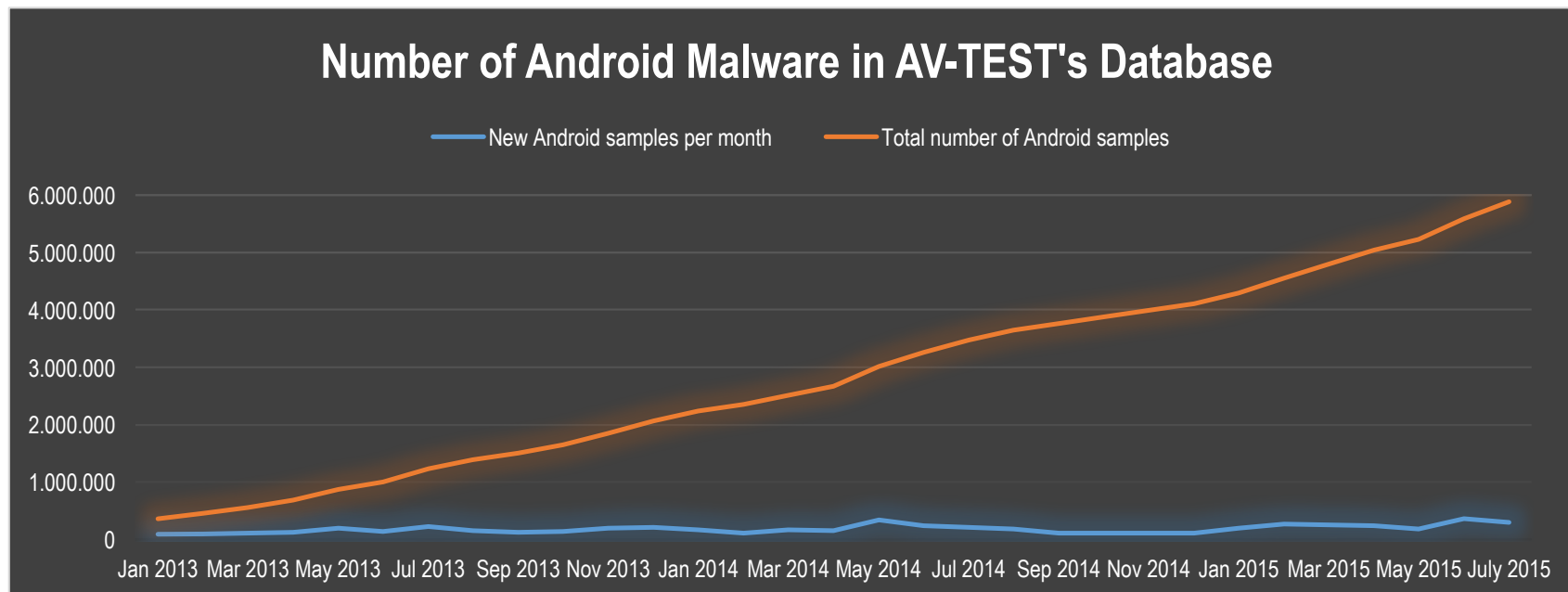
Wearable tech numbers used for personal injury claim

Fitbit data increasingly used as court evidence

Police: Woman's fitness watch disproved rape report

Warum haben sie Interesse an den Daten?

- University of Illinois: Verwendung einer **selbst geschriebenen App** zusammen mit der **Samsung Gear Live** war es möglich begründete Vermutung darüber anzustellen was geschrieben wurde <https://www.ece.illinois.edu/newsroom/article/11762>
 - Damit war es quasi möglich **Passwörter** zu **erraten**
 - **Android malware** ist im Kommen – Könnte auch so etwas ausnutzen



Wie erlangen sie Zugriff auf die Daten?

- **AV-TEST** hat die Sicherheit von **16 Fitness-Trackern** evaluiert

- <https://www.av-test.org/en/news/news-single-view/test-fitness-wristbands-reveal-data/>
- https://www.av-test.org/fileadmin/pdf/avtest_2015-06_fitness_tracker_english.pdf
- <https://www.av-test.org/de/news/news-single-view/7-fitness-armbaender-und-die-apple-watch-im-security-check-2016/>

- Auswahl nach **Bekanntheit, Verbreitung** und als Repräsentant eines **Preissegmentes**

- Gerät und dazugehörige **Android Applikation** analysiert

Produkt	App & Version
Acer Liquid Leap	
Leap Manager	1.0.292p
Basis Peak	
Basis Peak	1.17.1
FitBit Charge	
Fitbit	2.4.2
Garmin Vivosmart	
Garmin Connect Mobile	2.11.2
Huawei TalkBand B1	
Huawei Wear	12.03.02.01.00
Huawei Wear	12.04.03.01.00
Jawbone Up24	
UP	4.2.0
Microsoft Band 2	
Microsoft Health	1.3.20213.1
LG Lifeband Touch FB84	
LG Fitness	2.5.23
Pebble Time	
Pebble Time	3.9.1-966-bc5f043
Polar Loop	
Polar Flow	2.1.0
Runtastic Moment Elite	
Runtastic Me	1.5.3
Sony Smartband Talk SWR30	
Lifelog	2.6.A.0.10
SmartBand Talk SWR30	3.0.0.102
SportPlus Q-Band	
i-gotU Life	1.2.1506.947
Striiv Fusion	
Striiv Activity Tracker	1.0.1024p
Withings Pulse O _x	
Health Mate	2.04.40
Health Mate	2.04.50
Xiaomi MiBand	
Mi Fit	1.8.441

Wie erlangen sie Zugriff auf die Daten?

- **Mehrheit** der Geräte hatte **Schwachstellen**, die den unauthorisierten **Zugang** oder die **Manipulation** zu Nutzerdaten zuließen
- **Alle Schwachstellen** wurden an die entsprechenden **Hersteller gemeldet**
 - **Fitbit** hat nach der **Zusammenarbeit** mit uns ein **Firmware-Update** herausgebracht, das zwei kritische **Schwachstellen gefixt** hat
 - Einige **Hersteller antworteten** überhaupt **nicht** → Viele der Geräte sind **immer noch verwundbar**

■ Bluetooth

- Mehrheit der Tracker implementiert **kein adäquates Pairing / Bonding**
 - Tracker sind **immer auffind-** und für beliebige Geräte **verbindbar**
 - Nutzer hat **keine Kontrolle** darüber, ob und mit welchen Geräten gerade eine **Kommunikation** stattfindet
 - **BLE Privacy Feature** nur in 2 Fällen angewandt

■ Datenspeicherung

- Mehrheit der Apps verlässt sich auf den **Zugriffsschutz von Android**
 - **Nutzerdaten** (teilweise mit Nutzerpasswort) liegen im **Klartext** im Appverzeichnis → **Problem auf gerooteten Geräten**
- Verwendung des freien Speicherbereichs (z.B. SD-Card) um **Log-files** und **temporäre Daten ungeschützt** abzulegen → **Zugriff von Dritt-Apps**

■ Authentifizierung

- Hohe **Anfälligkeit** für **Replay**-Attacken
 - Viele Tracker arbeiten mit **festem Auth-Befehl**
 - Selbst scheinbar randomisiert berechnete funktionieren **beliebig oft**
- **Unvollständige** Authentifizierung
 - **Wichtige Funktionen** von Authentifizierung **ausgenommen**
 - Authentifizierung **in Programmablauf zu spät**
- **Fehlende** Authentifizierung
 - Teilweise ist sogar die **Nutzung eines Trackers** mit **mehreren Accounts** möglich (Data sharing)

■ Datenübermittlung zur Cloud

- Grundsätzlich keine (wirklichen) Probleme feststellbar
 - **Sensible Kommunikation** bei allen getesteten Apps **über gesicherte Kanäle**
 - Allerdings relativ **häufig** besteht **Anfälligkeit gegen Man-in-the-Middle-Attacken**, was Mitlesen und Manipulation durch Dritte erlaubt

■ Schutz gegen Reverse Engineering

- Etwa 50% aller Apps setzen keine oder **keine adäquate Obfuscation** ein
 - **Reverse Engineering erheblich erleichtert** und damit Aufwand für Angriff deutlich gesenkt
- Einige Apps im vollständigen oder teilweisen **Debug-Status** ausgeliefert
 - Beinhalten noch **Debug-Ausgaben**
 - Legen Debug **Log-files** an
 - Ausführliches **Logcat-Logging**

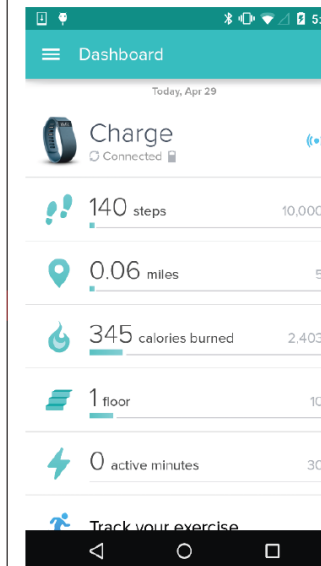
Ausgewählte Beispiele - *Fitbit Charge*

■ Live-Data

- „Feature“
- Liefert **Fitnessdaten ohne Authentifizierung**
- Aktivierbare **Notifizierungen** erlauben Erhalt der Daten in (beinahe) **Echtzeit**

FIXED!

```
1 // ... Initialize Bluetooth LE scanning via standard Bluetooth LE protocol
2 // ... Establish connection to "Charge" via standard Bluetooth LE protocol
3 // ... Discover services running on tracker via standard Bluetooth LE protocol
4
5 public void onServicesDiscovered(BluetoothGatt gatt, int status) {
6     //Fitness data service; UUID from service discovery
7     BluetoothGattService service = gatt.getService(UUID.fromString("558dfa00-4fa8-4105-9f02-4eaa93e62980"));
8
9     //Enable notifications to retrieve fitness data whenever it has changed;
10    BluetoothGattCharacteristic serviceCharacteristic = service.getCharacteristic(UUID.fromString("558dfa01-4fa8-4105-9f02-4eaa93e62980"));
11
12    setCharacteristicNotification(gatt, serviceCharacteristic, true);
13    // ... Be notified whenever updated fitness data is available
14 }
15
16 public void onCharacteristicChanged(BluetoothGatt gatt, BluetoothGattCharacteristic characteristic) {
17     //Fetch the data
18     byte[] data = characteristic.getValue();
19 }
```



12 A3 40 55 8C 00
steps

00 00 F0 8B 01 00
floor

59 01 0A 00 00 00
calories

■ Steuerung/Manipulation/Auslesen

- **Steuerungsbefehle** direkt über **00002aff-0000-1000-8000-00805f9b34fb** geschrieben

- Von jedem **beliebigen Smartphone** das Verbindung aufbauen kann

■ Steuerbefehle

- 00 00 00 70 D5 01 **70 17** **A4 06** **46 00** **19** 00 10 0E
00 00 1B 00
Gewicht in g/10 Schrittweite in cm
Größe in cm*10 Alter
- 00 00 00 71 **FF FF FF FF FF FF FF FF** **00 00 00 00**
00 00 00 00
Weckzeiten in min Wiederholungen
- 00 00 00 72... - Daily Goals
- 00 00 00 73-76... - Alarm Labels
- 1F 00 80 16 - Factory Reset

- **Fitnessdaten** von Characteristic **00002a53-0000-1000-8000-00805f9b34fb**

- Einfache **Notifizierung** des Chars **genügt für Erhalt** in Form von 18 Byte Feld mit Daten inklusive Schritte, Kadenz, Geschwindigkeit, Distanz, Kalorien...

■ Manipulation

- User-Infos zu Größe, Gewicht, Schrittlänge lassen sich auf mehr als **unrealistische Werte** ändern
- Sogar über die **Original-App** möglich
- Werte werden **ohne Plausibilitätstest** für die **Berechnung** der zurückgelegten **Strecke** und verbrannten **Kalorien** verwendet

07-07 07:57:02.270 19725-19725/de.avt.bluesearch l/native-activity: JNI updating user profile

07-07 07:57:02.270 19725-19725/de.avt.bluesearch l/native-activity: JNI Updating user to user with ID 356291

07-07 07:57:02.270 19725-19725/de.avt.bluesearch l/native-activity: JNI updating name SHSK.avt@googlemail.com, ID 356291, user weight is 14121.300000, height is 7866.929170, stride is 9027.708676, units is 0, lang is 3, custom is

- Von Characteristic **0000fff1-0000-1000-8000-00805f9b34fb** erhält man dann Fitnessdaten

	Gegangene Schritte				Gelaufene Schritte				Aktive Zeit				Distanz			
■	FF	F1	07	00	01	CC	00	02	28	00	00	00	08	02	C5	D8
	03	CA	00	00	05	62										

Kalorien

- Also: 460 Schritte gegangen, 552 Schritte gelaufen, **8min** dafür aufgewandt, **2,9 Meilen** zurückgelegt und dabei 970 Kalorien verbrannt (Weltrekord 5000m: 12,37:35min)

Wie erlangen sie Zugriff auf die Daten?

- Warum ist das so?
 - Hersteller sehen oft **keine Notwendigkeit für Sicherheitsbetrachtungen** („Why would anyone hack a fitness tracker?“)
 - Viele Hersteller kommen aus ursprünglich gänzlich anderen Produktparten und ihnen **fehlt** daher schlicht das **Know-How**
 - Selbst wenn sie versuchen Sicherheitsmechanismen zu implementieren **scheitern** sie
 - **Alte Fehler** aus der klassischen Informatik wiederholen sich **immer und immer wieder**:
 - **Keine Authentifizierung** oder fehlerhafte Implementation
 - **Keine Verschlüsselung** oder fehlerhafte Implementation
 - Fehler, die man in der klassischen Informatik seit **10-15 Jahren** nicht mehr sieht
 - **Enge Deadlines**, Marktanforderungen, **Features** haben immer höchste Priorität
 - Allerdings ist die Umsetzung eines **Sicherheitskonzeptes** ab der **Planungsphase** an deutlich günstiger als das nachträgliche Fixen, Updaten und Patchen

- Sollten Nutzer vollständig **auf Fitness-Tracker verzichten?**
 - **Nein**, aber sie sollten sich dem potentiell **gravierenden Einschnitt** in ihre **Privatsphäre** und den **möglichen Gefahren** bewusst sein
 - Es gibt tatsächlich auch einige **Geräte**, die ein **solides Sicherheits- und Datenschutzkonzept** aufweisen
 - Derzeitig sind **noch keine großangelegten realen Angriffe** auf Fitness-Tracker bekannt
 - Aber: Sobald es für die Daten einen Markt gibt, wird es auf jeden Fall versucht werden (siehe Internet of Things)
- Sollten **Versicherungen** tatsächlich Tarife und Rabatte von Fitnessdaten abhängig machen?
- Sollten Fitness-Tracker als **Beweismittel vor Gericht** zugelassen sein?
- Die **Entwicklung** ist hier **erst am Anfang** → Unternehmen und Kriminelle werden neue Wege finden Nutzen aus diesen Daten zu ziehen
- Potential für **DAS Überwachungswerkzeug** schlechthin
- **“Daten sind die Ressource der Zukunft”**



Vielen Dank für Ihre Aufmerksamkeit!