

IT-Sicherheit in smarten Gebäuden

Bundesverband IT-Sicherheit e.V. (TeleTrust) in Kooperation mit
SmartHome Initiative Deutschland e.V.

Berlin, 29.10.2019

Ziemlich smart. Aber auch sicher?

Zur aktuellen Gefahrensituation bei IoT-Geräten und Diensten

Olaf Pursche, AV-TEST Institut



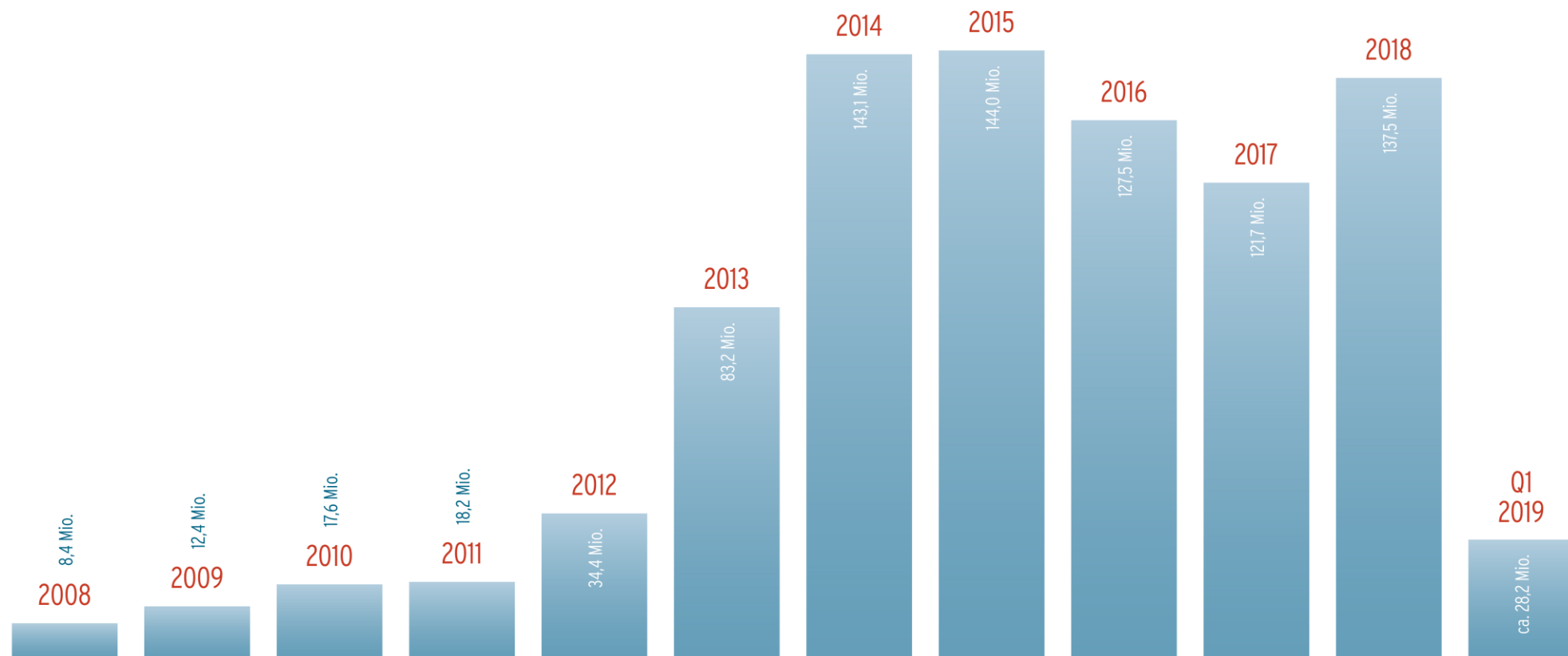
The Independent IT-Security Institute

Magdeburg Germany



- MEHR ALS 30 IT-SPEZIALISTEN
- MEHR ALS 15 JAHRE EXPERTISE IM BEREICH ANTIVIREN-FORSCHUNG
- UNTERNEHMENSGRÜNDUNG 2004
- **EINE DER GRÖßTEN VIREN-DATENBANKEN DER WELT**
- **500 CLIENT- UND SERVER-SYSTEME**
- **2.500 TERABYTE TESTDATEN**
- **MEHR ALS 5.000 EINZEL- UND VERGLEICHSTESTS PRO JAHR**
- ANALYSE, TESTING, DEVELOPMENT, CONSULTING & SERVICES
FÜR AV-HERSTELLER, FACHMAGAZINE, BEHÖRDEN UND UNTERNEHMEN

Entwicklung neuer Malware insgesamt in den letzten 10 Jahren



WTFEST

The Independent IT-Security Institute

Magdeburg Germany



WEST

The Independent IT-Security Institute

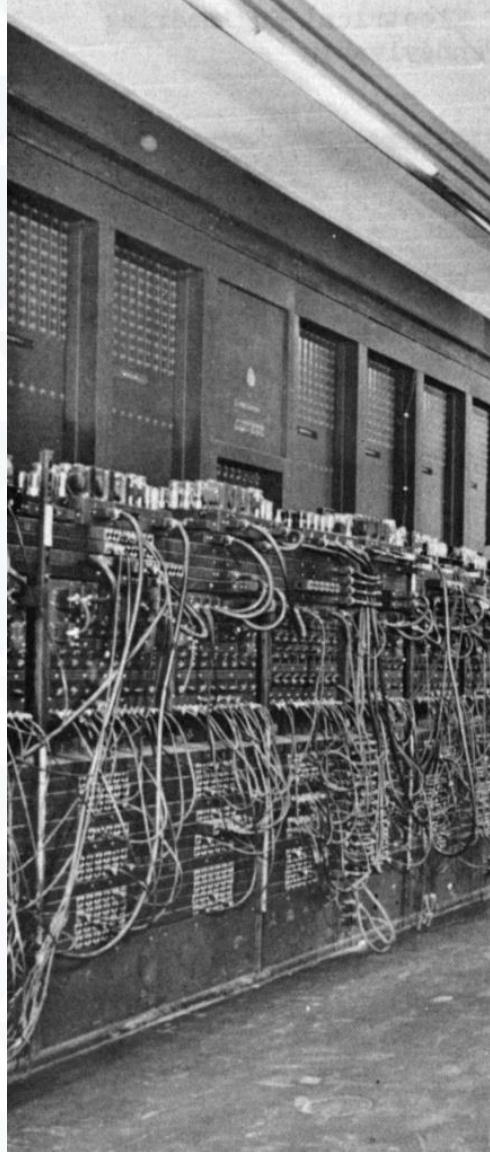
Magdeburg Germany





The Independent IT-Security Institute

Magdeburg Germany

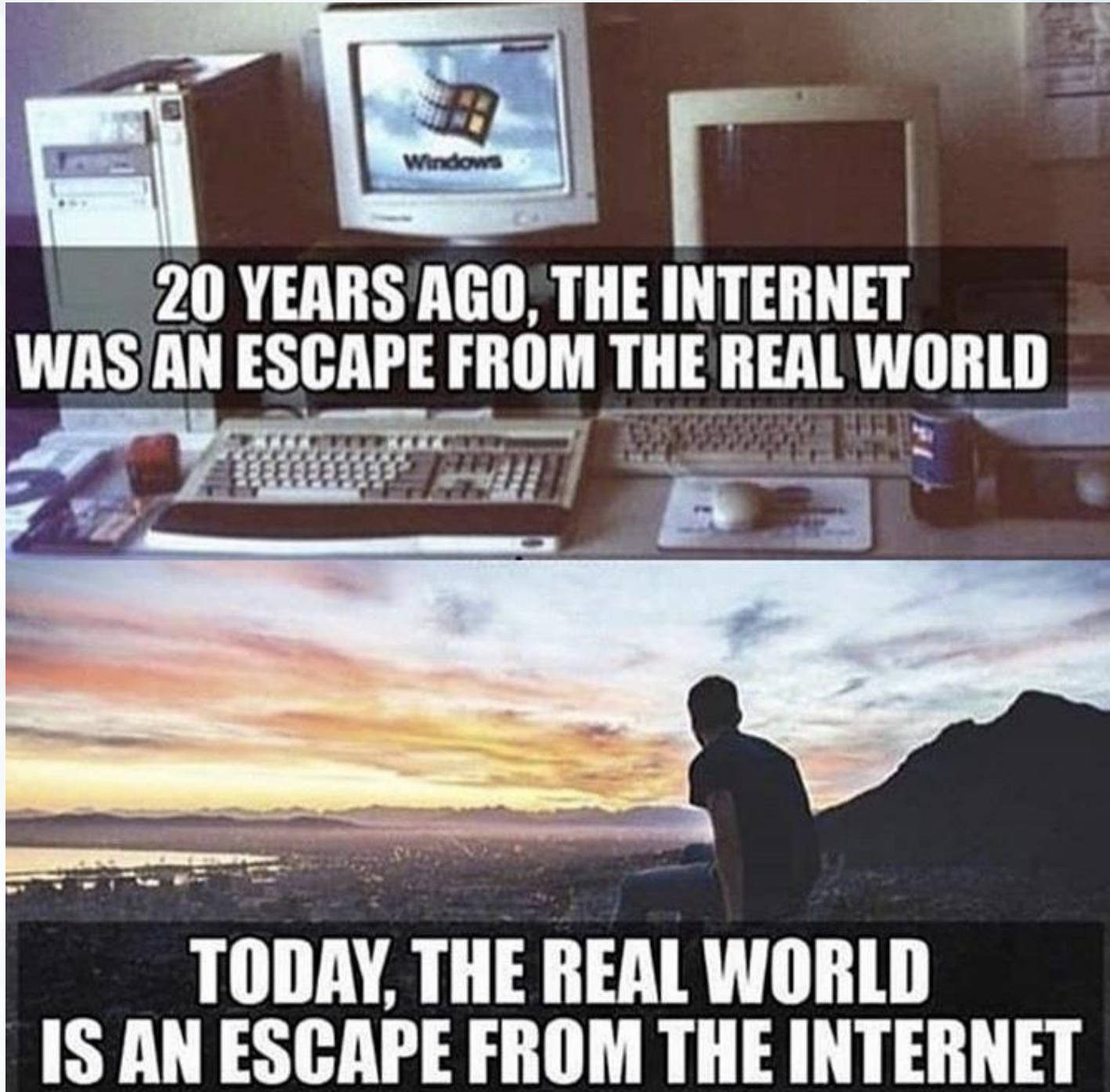


Quellen: Wikipedia & Apple



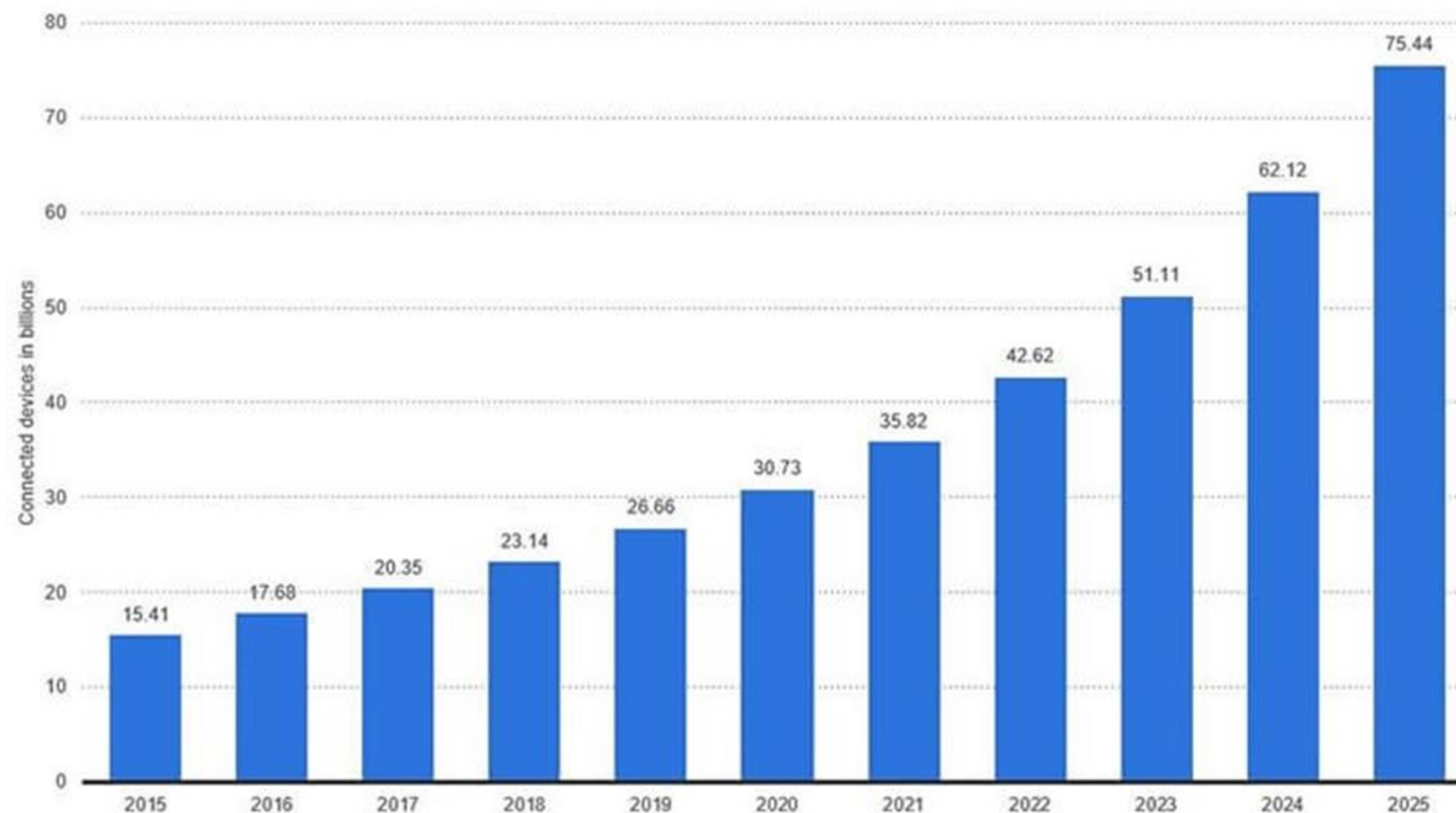
The Independent IT-Security Institute

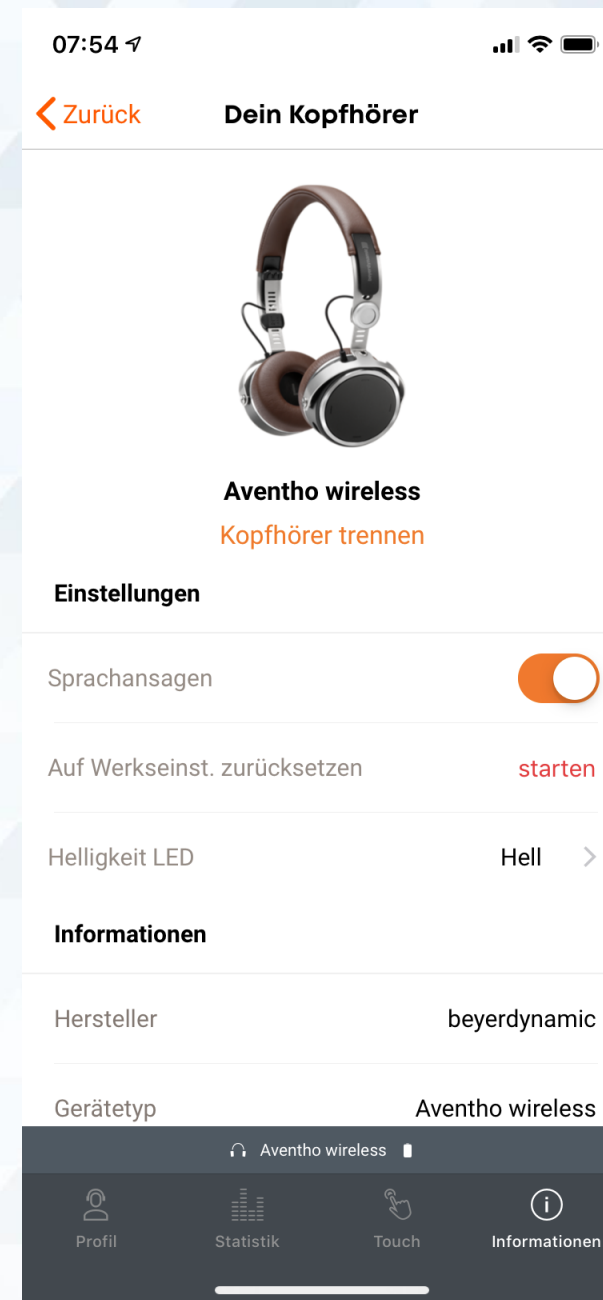
Magdeburg Germany



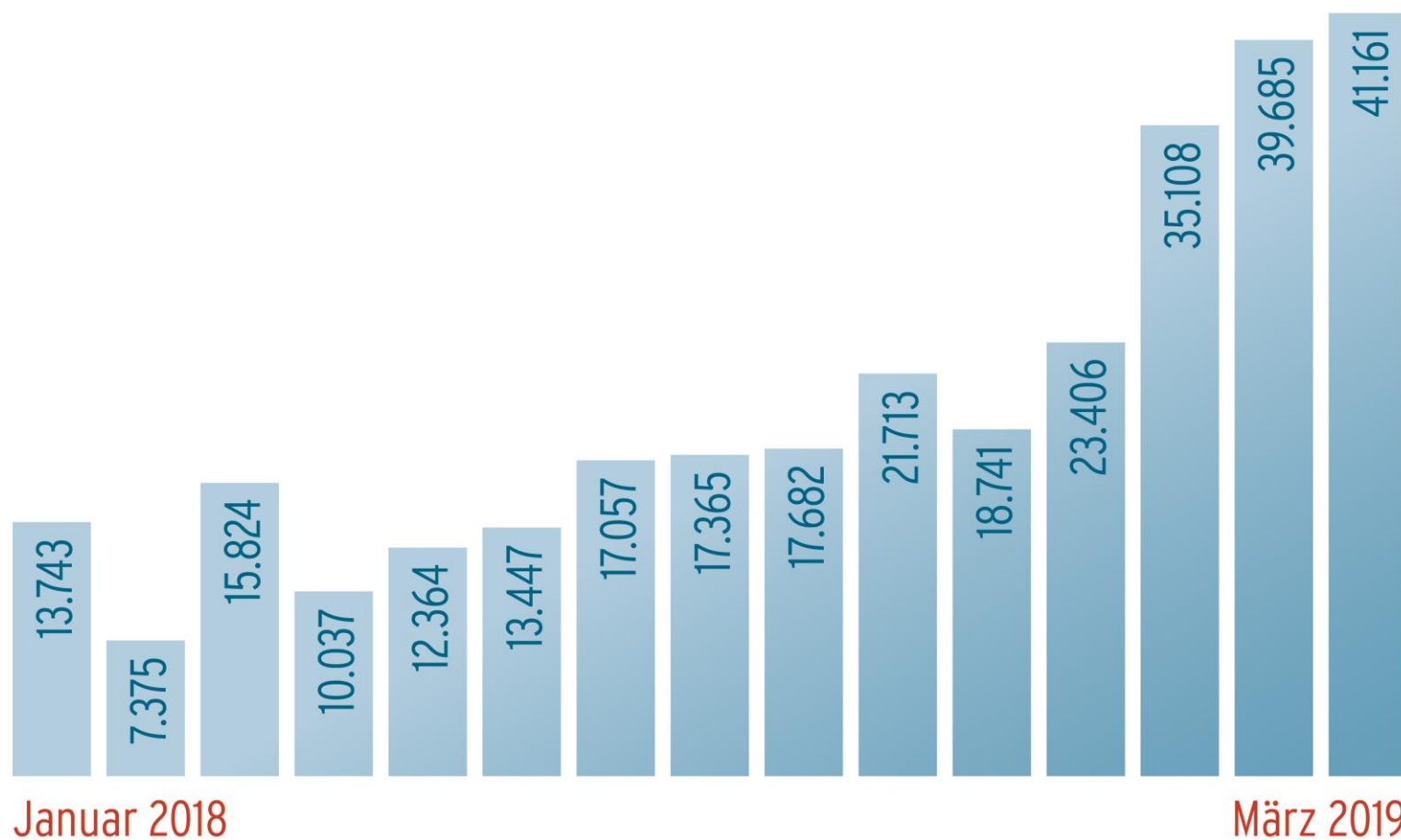
Internet of Things - number of connected devices worldwide 2015-2025

Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)

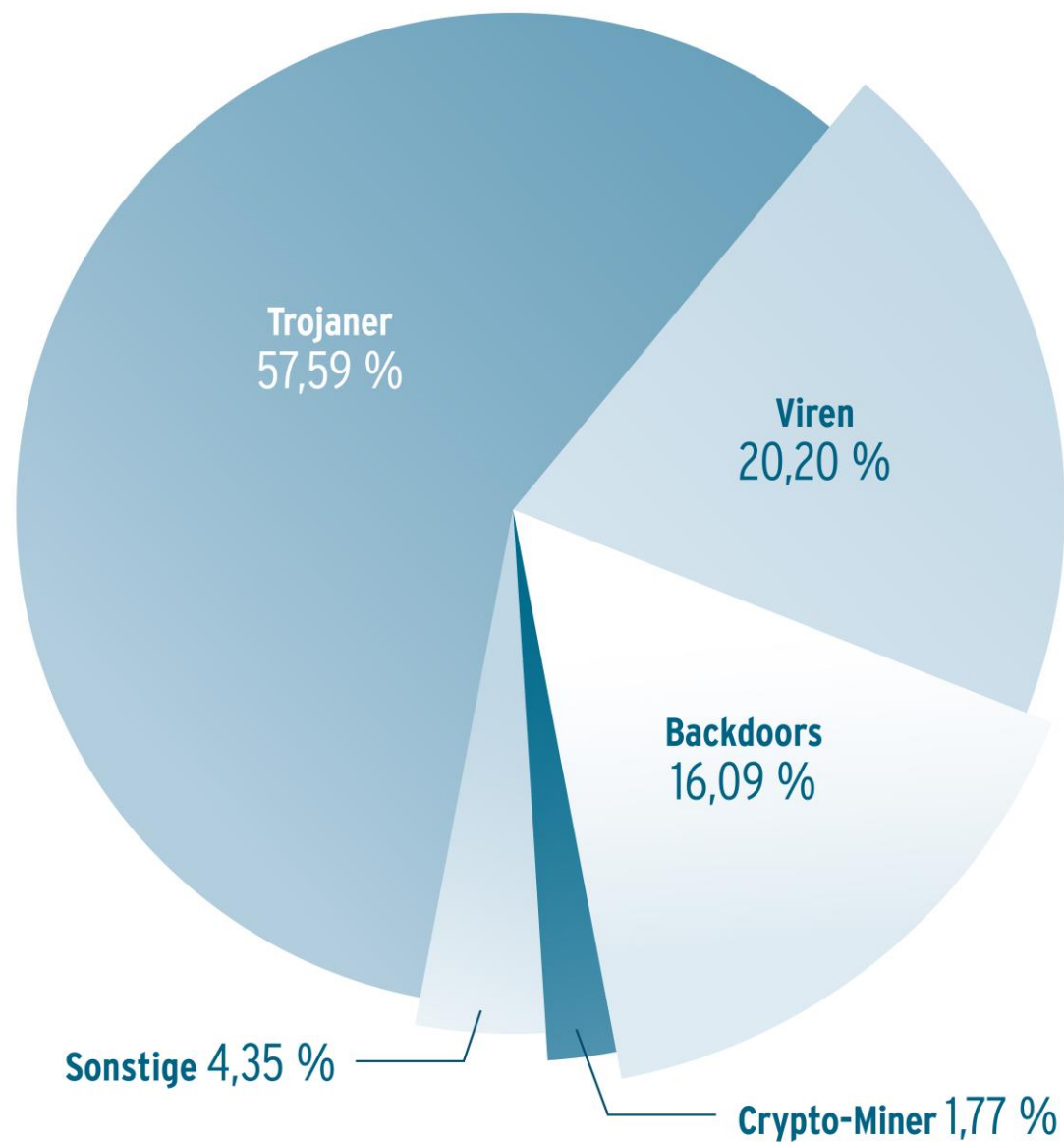


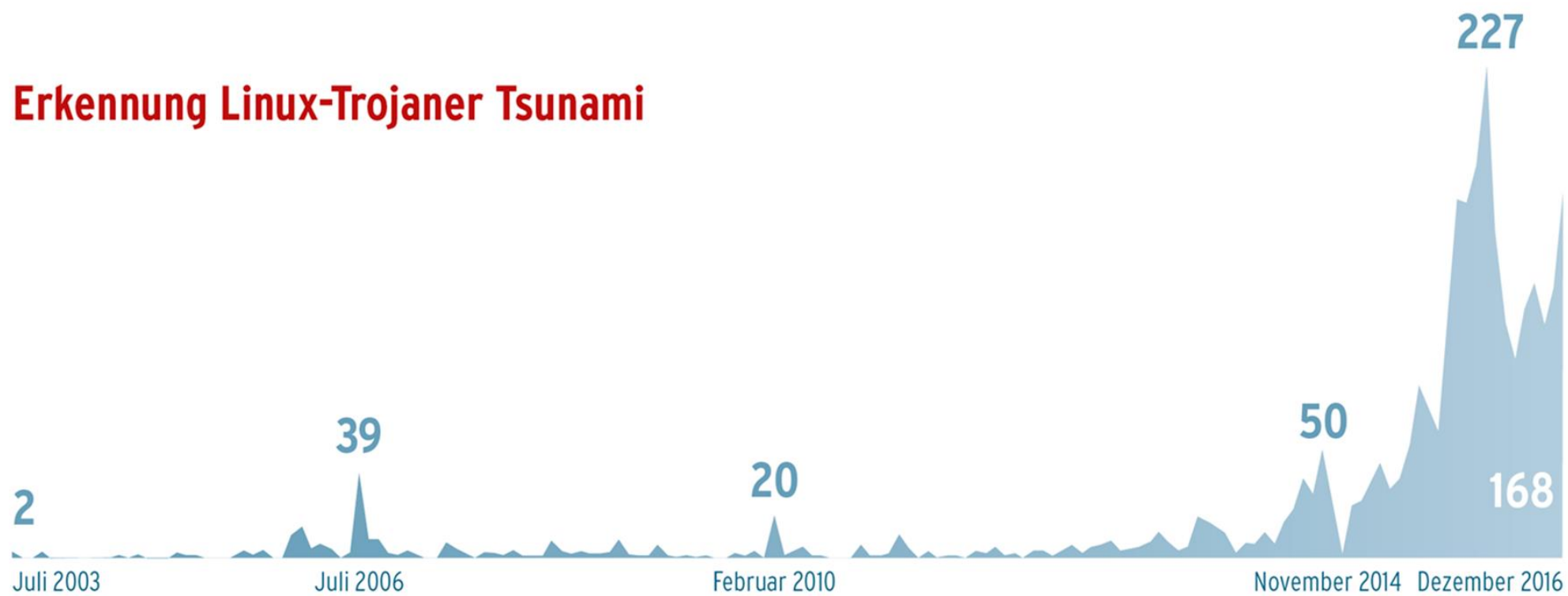


IoT/Linux: Entwicklung neuer Malware insgesamt 2018 + Q1 2019



IoT: Malware-Verteilung 2018

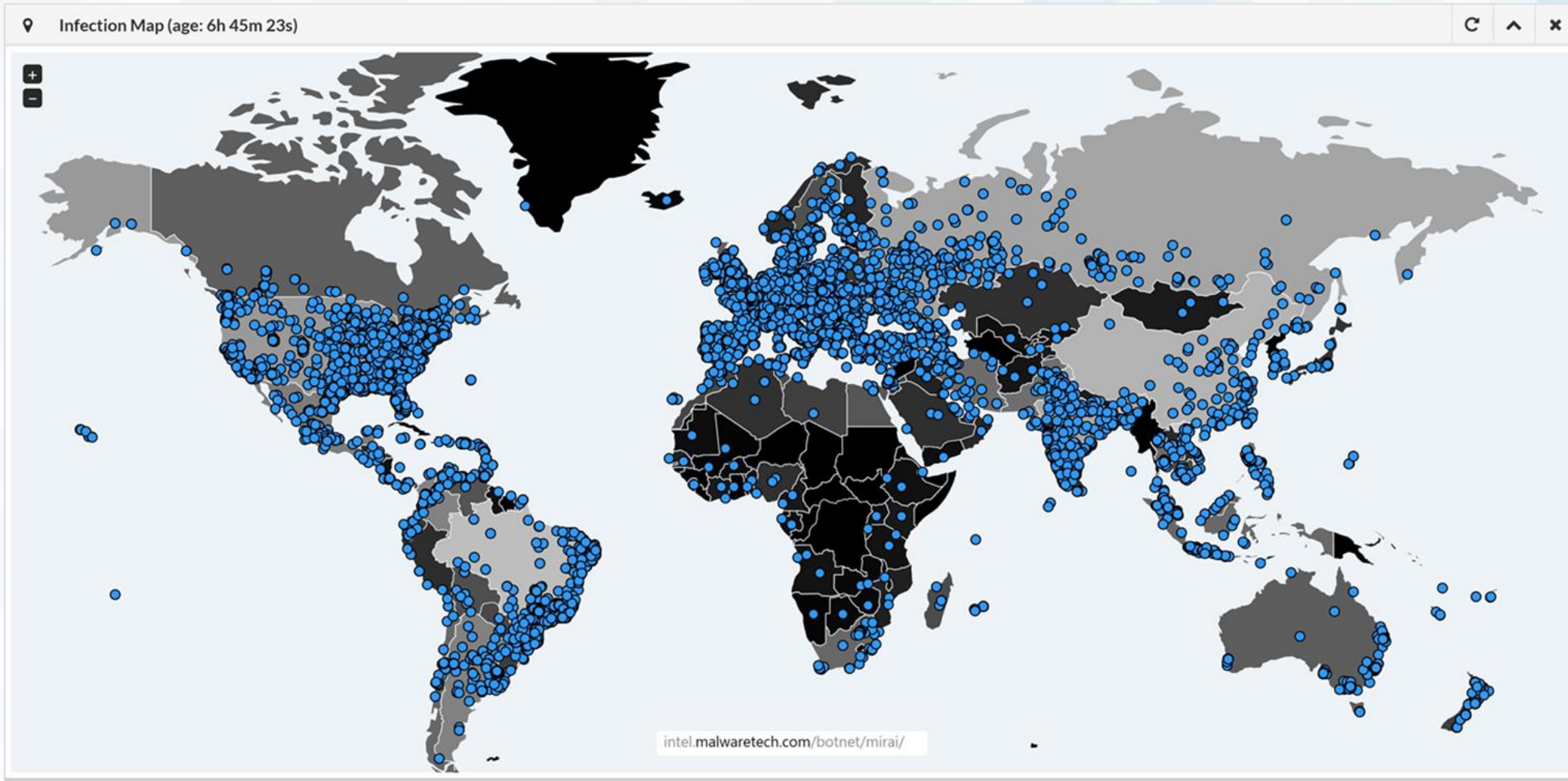




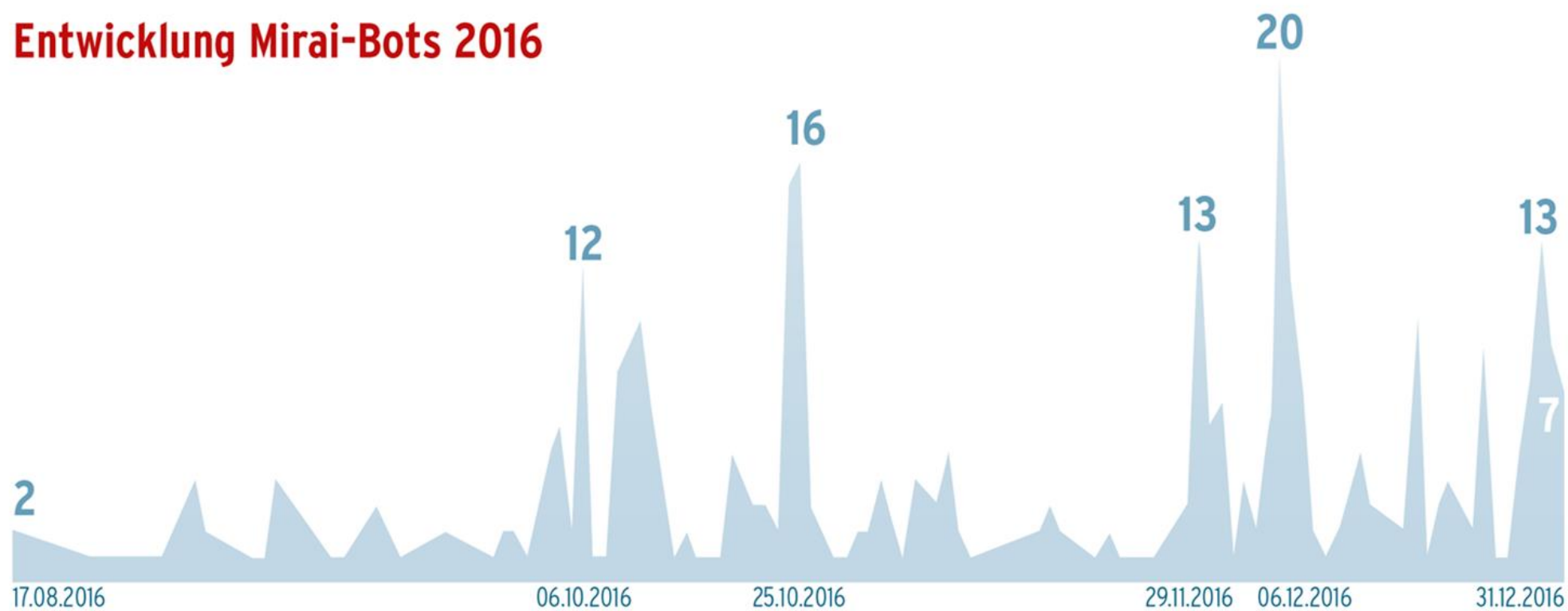


The Independent IT-Security Institute

Magdeburg Germany



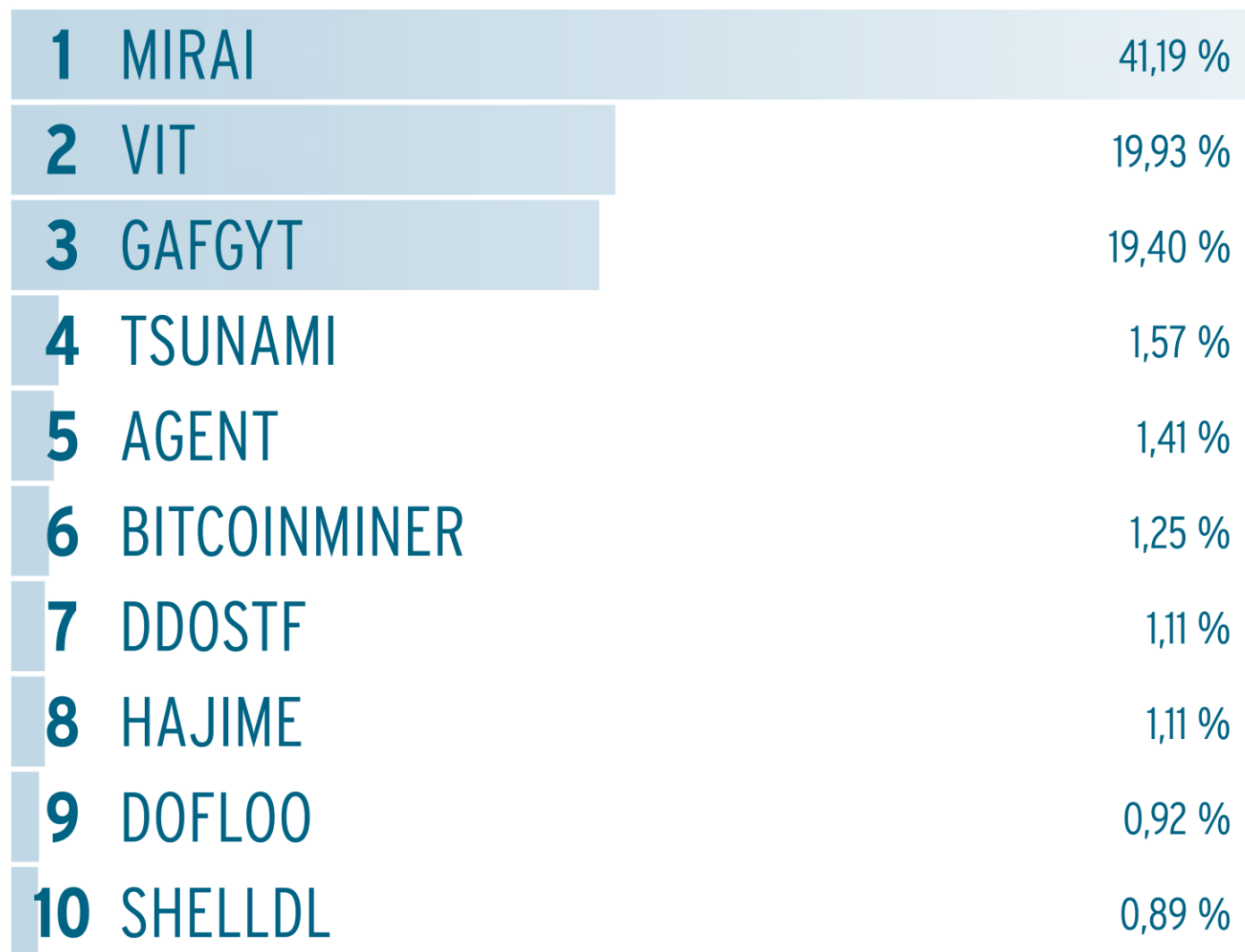
Entwicklung Mirai-Bots 2016

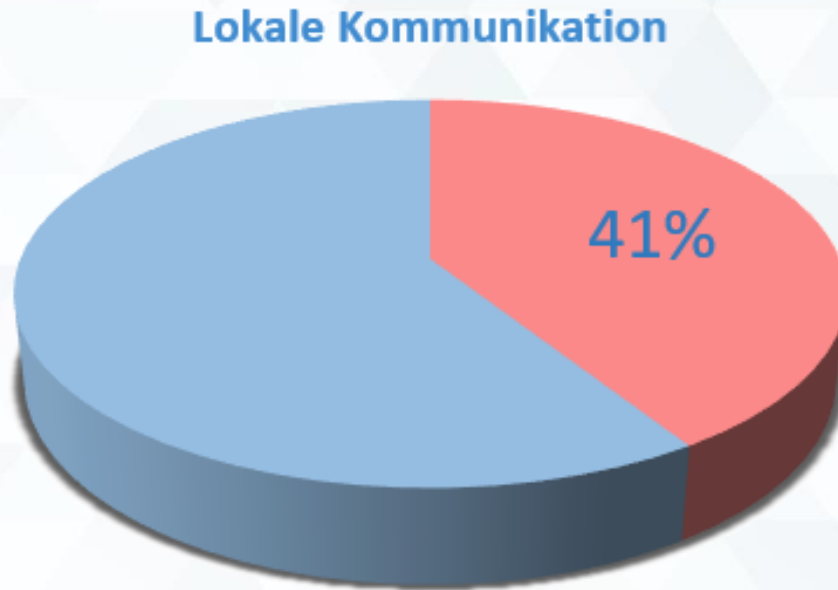


IoT: Entwicklung neuer Mirai-Trojaner 2018 + Q1 2019



TOP 10 IoT-Malware 2018

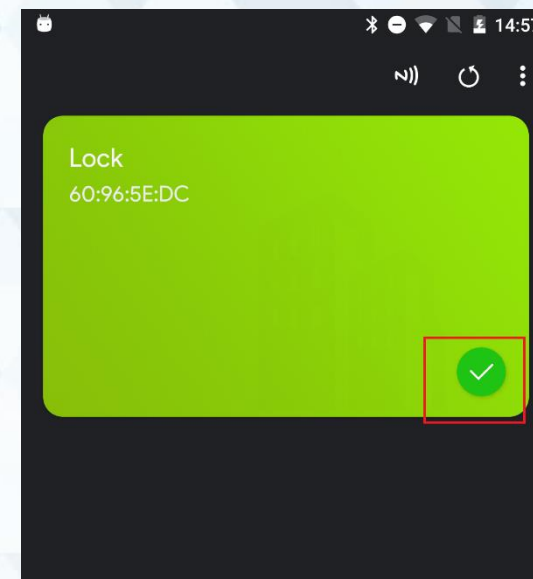
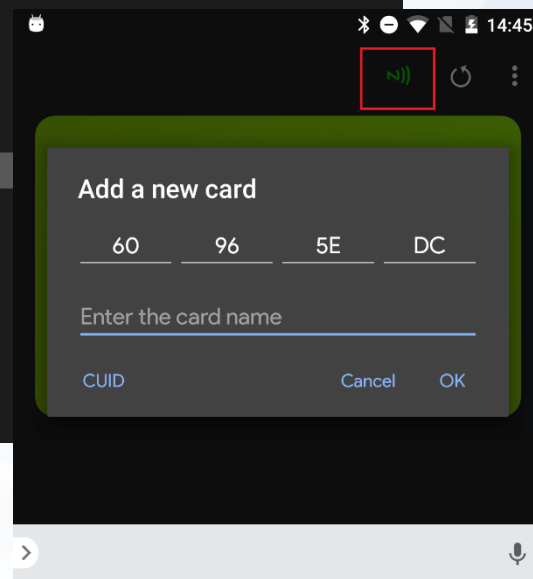




- Alle Offline-Kommunikation, die zwischen Systemkomponenten und dem Smartphone stattfindet (bspw. per LAN, Bluetooth, NFC, ...)
- Oft aufgrund falscher Sicherheitsannahmen und/oder zur Aufwandseinsparung vernachlässigt
- Hauptsächlich Probleme bei **Authentifizierung** und **Verschlüsselung**

```
2018-09-05 11:43:46 POST https://192.168.82.12/cgi-bin/devm_request.cgi
← 200 OK application/json 27b 94ms

Request Response Detail
Accept: application/json
Content-type: application/json
Content-Length: 130
Host: 192.168.82.12:443
Connection: Keep-Alive
Couldn't parse: falling back to Raw
sipnum=dc9886aa38f2@6772021282405758&request={
  "request": 202,
  "inHouse": true,
  "data": {
    "armMode": 1
  }
}
```



```
GET /local/Doorcom/getuser.cgi?u=ghetsk0001&p=k3cdwegcwZ&format=json HTTP/1.1
```

```
Connection: close
```

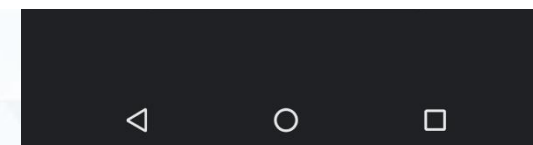
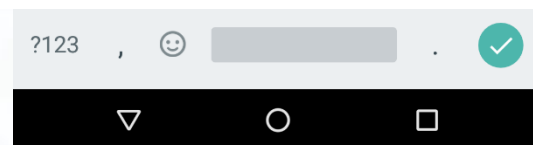
```
User-Agent: DoorBirdApp/4.60 (54; Motorola moto g(7); Android 9; de-DE) Dalvik/2.1.0 (Linux; U; Android 9; moto g(7) Build/PPOS29.80-66-2)
```

```
Authorization: Digest username="ghetsk0001", realm="DoorBird Station", nonce="5d512d6c:a06f484df9f08d438dbfe7530a6d5bfb", uri="/local/Doorcom/getuser.cgi?"
```

```
u=ghetsk0001&p=k3cdwegcwZ", qop="auth", nc=00000001, cnonce="dYJfP3b4jp5JWjHr", response="67a69f82d0b7f399231db67c85135244", algorithm=MD5
```

```
Host: 192.168.82.20
```

```
Accept-Encoding: gzip
```





© by Pearl

Neueste Tests, Smart Home

Pearl Harbor: Sicherheitswarnung für Smartlock VisorTech TSZ-580.f



August 15, 2019

Olaf Pursche

„Nie wieder ausgesperrt: Denn Sie schließen Ihre Haustür einfach per Fingertipp auf! Alternativ öffnen Sie Ihr Türschloss per Smartphone-App oder Transponder“, bewirbt VisorTech sein Smart Lock. Doch leider funktioniert das Öffnen des Smart Locks all zu einfach. Um Türen, in denen das VisorTech-Schloss verbaut ist zu öffnen, brauchen Angreifer nur die unverschlüsselt auf dem mitgelieferten Transponder gespeicherten Zugangsdaten mit einer Gratis-App zu kopieren, schon öffnet das Smartphone fremde Türen. Auf den Hinweis zur Unsicherheit des Transponders durch das AV-TEST Institut hat Pearl mittlerweile reagiert und will neue Schlösser mit Transpondern ausstatten, bei

Kategorien

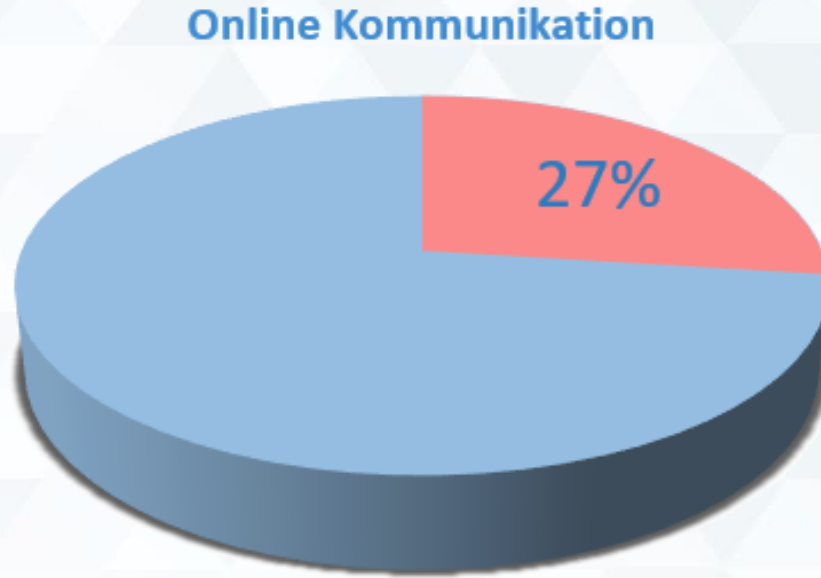
Allgemein ▶

Allgemeine Information ▶

Automobil ▶

eHealth ▶

Gadgets ▶



- Alle Online-Kommunikation zwischen Systemkomponenten und der mobilen Applikation und der Cloud
- In den meisten Bedrohungsszenarien die **Toppriorität**, da naturgemäß das häufigste Einfallstor
- Oft Probleme bei Verschlüsselung und Implementation dieser (Zertifikatsvalidierung und Anfälligkeit für MitM-Angriffe)
- Unsichere Web-APIs



- TATORT MÜNCHEN, 2.12.2018 „WIR KRIEGEN EUCH ALLE“, LENA MIT SMARTER PUPPE SENTA

Internet

CloudPets stuffed toys leak details of half a million users

Company's data compromised, leaking information including email addresses, passwords and voice recordings

Alex Hern

@alexhern

Tue 28 Feb 2017

14.59 GMT



This article is over 1 year old



most viewed



Barack Obama lambasts Trump over legal troubles



Labour could seize option of second Brexit vote, says McDonnell



'A humiliation': Outcry after Mexico president gives highest honour to Jared Kushner



UK significantly worse off under all Brexit scenarios - official forecast



Live May accused of having 'head in sand' over Brexit making UK poorer - Politics live



The Independent IT-Security Institute

Magdeburg Germany

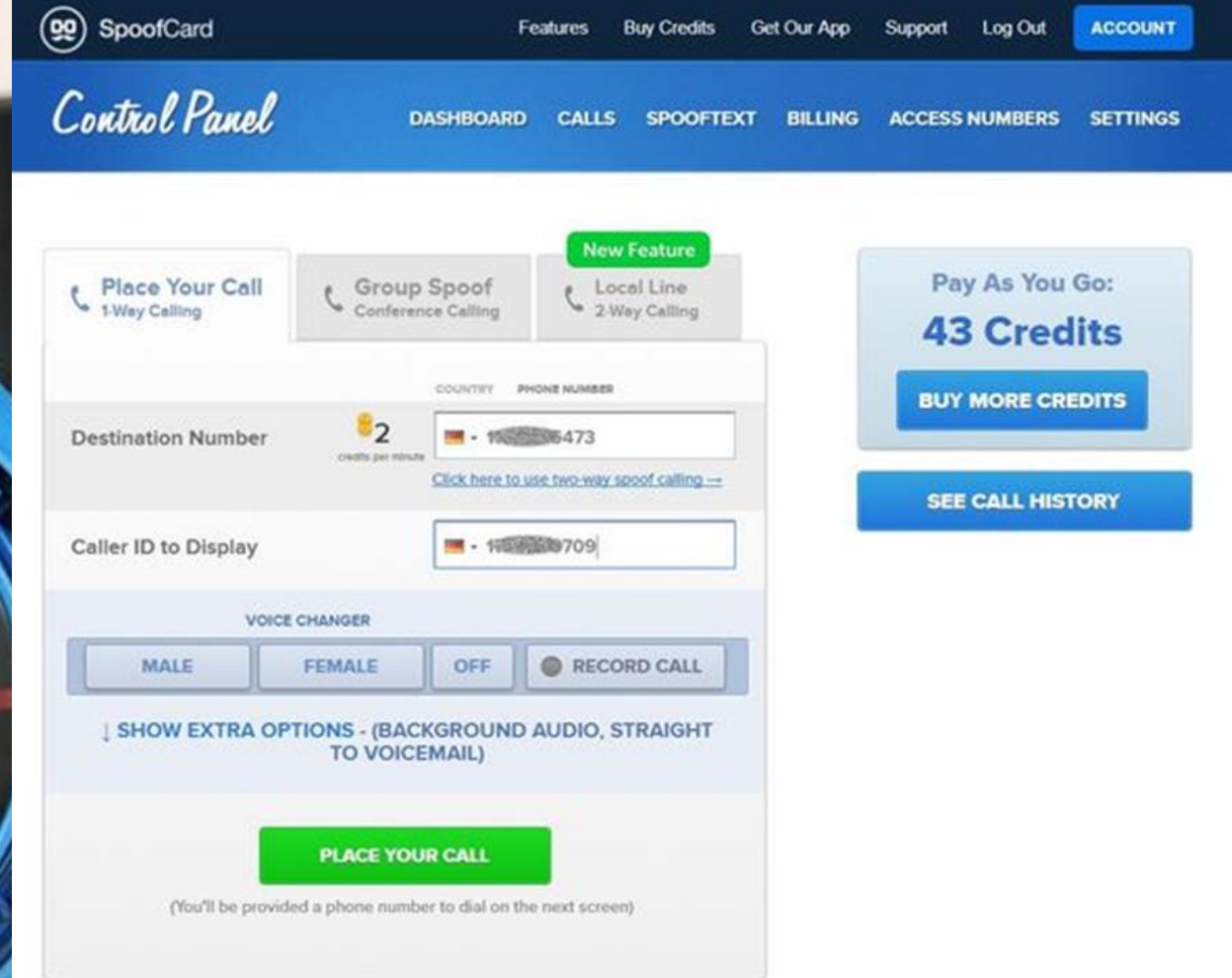




TEST

The Independent IT-Security Institute

Magdeburg Germany



METHOD
POST

HEADERS
☒ Content-Type: application/json
[+ Add header](#)

52.1135139, 11.6207104

52°06'48.7"N 11°37'14.6"E

52.113514, 11.620710

Routenplaner

Speichern

In der Nähe

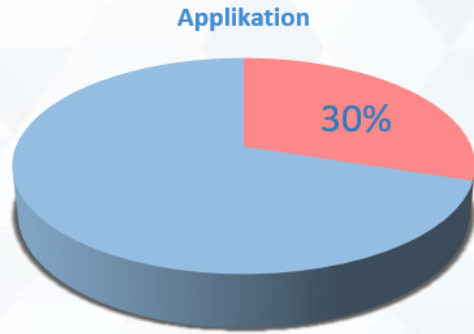
An mein Smartphone senden

Teilen

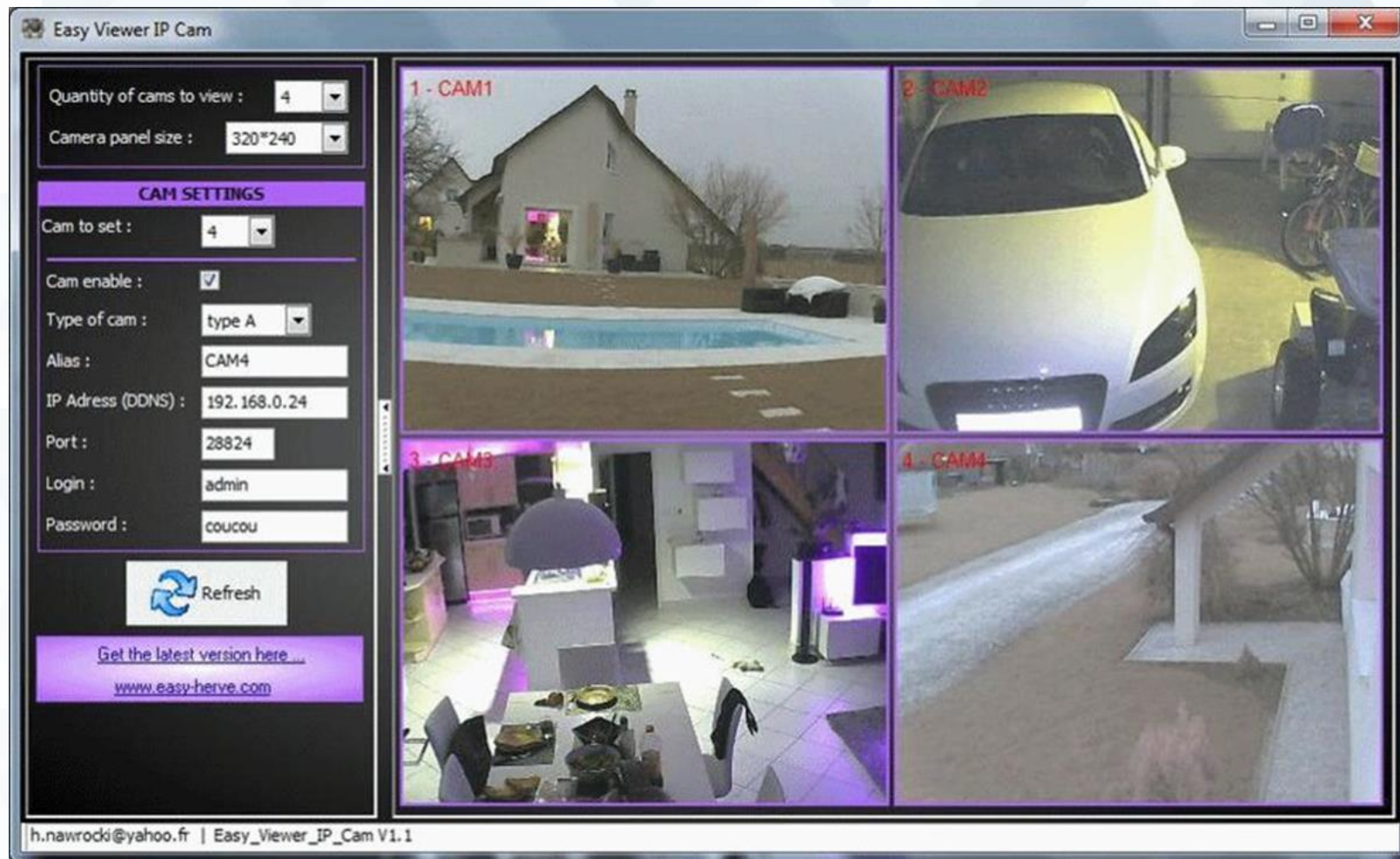
Klewitzstraße 8, 39112 Magdeburg

4J7C+C7 Magdeburg





- Sicherheitsrelevante Aspekte in Konzept und Implementation der zum Produkt gehörigen mobilen Applikation und Firmware
- Häufigste Probleme sind Implementationsfehler der verschlüsselten Kommunikation, hard-coded secrets und Schwachstellen in Third-Party Modulen
- Nicht dokumentierte und/oder nicht abgesicherte Fernzugänge
- Gerade auf **Android** ist das Reverse-Engineering meist unkompliziert und Schwachstellen treten dadurch leichter ans Tageslicht



■ INSECAM

- Weltweit größtes **Online Camera Directory**
- **Streams** ungesicherter Kameras und Direktzugriff zu Konfigurationsmenüs

https://www.insecam.org/en/bycountry/DE/?page=12

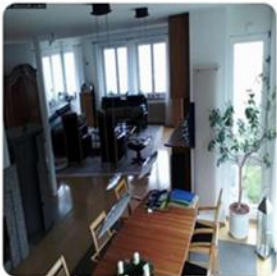
Suchen

IP cameras: Germany

f Facebook t Twitter + More

IT Wartung für EMC Post Warranty - End of Life Wartung Allera Service for IT mehr Infos

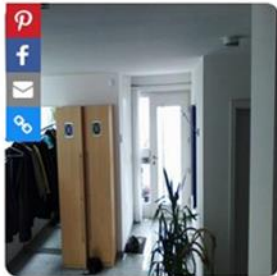
« 1 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 ... 114 »



Watch Vivotek camera in Germany,Nuremberg



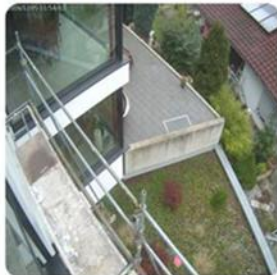
Watch Vivotek camera in Germany,Ruttenscheid



Watch Vivotek camera in Germany,Nuremberg



Watch Vivotek camera in Germany,Karlsruhe



Watch Vivotek camera in Germany,Karlsruhe

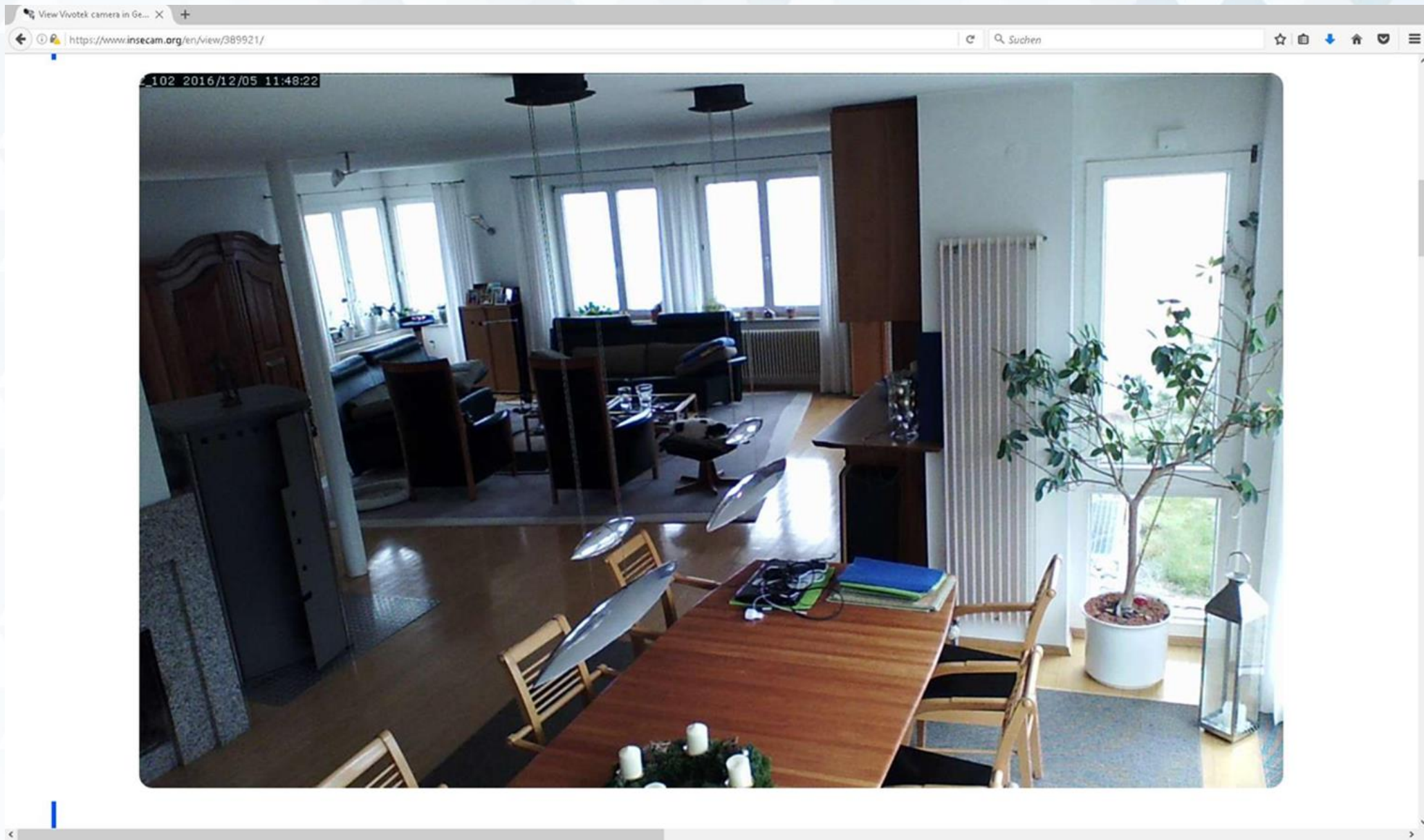


Watch Vivotek camera in Germany,Hamburg

WTEST

The Independent IT-Security Institute

Magdeburg Germany



WTFEST

The Independent IT-Security Institute
Magdeburg Germany

View Vivotek camera in Ge... X +

https://www.insecam.org/en/view/389921/ Suchen



Make Your Photos Amazing
Apply Makeup To Your Portraits! Get New Version 15 now. Go to portraitprofessional.com

Country: Germany. You can see other [online cameras](#) in Germany.
Country code: DE
Region: Bayern
City: Nuremberg. [View CCTV online](#) in Nuremberg.
Latitude: 49.447780
Longitude: 11.068330
ZIP: 90455
Timezone: +01:00
Manufacturer: Vivotek



View larger map

Powered by Google

NOTE: The coordinates are very approximative and have accuracy in hundreds of miles



The Independent IT-Security Institute

Magdeburg Germany

File Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

Login Insecam - World biggest o... mirai-infection-map.jpg (JPEG... +

187.138.188.28 botnet mirai

Any time & Any where

IP Surveillance for Your Life



Customer Login

Username : admin

Password :

Verify Code : 2SE3

2SE3

LOGIN

View: [Mobile](#) | PC



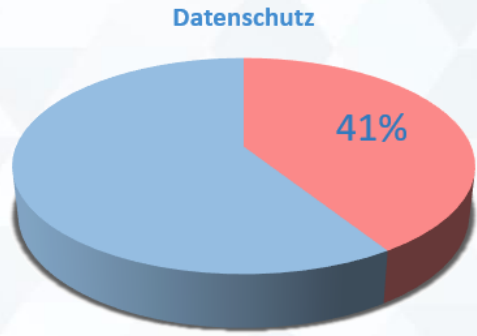


The Independent IT-Security Institute

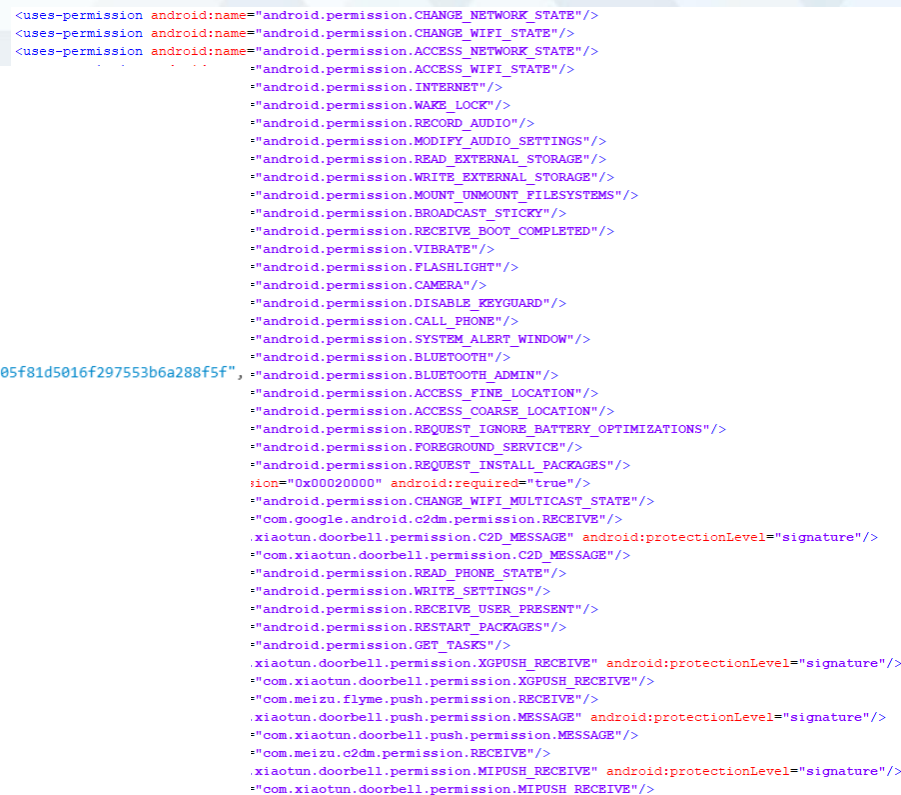
Magdeburg Germany

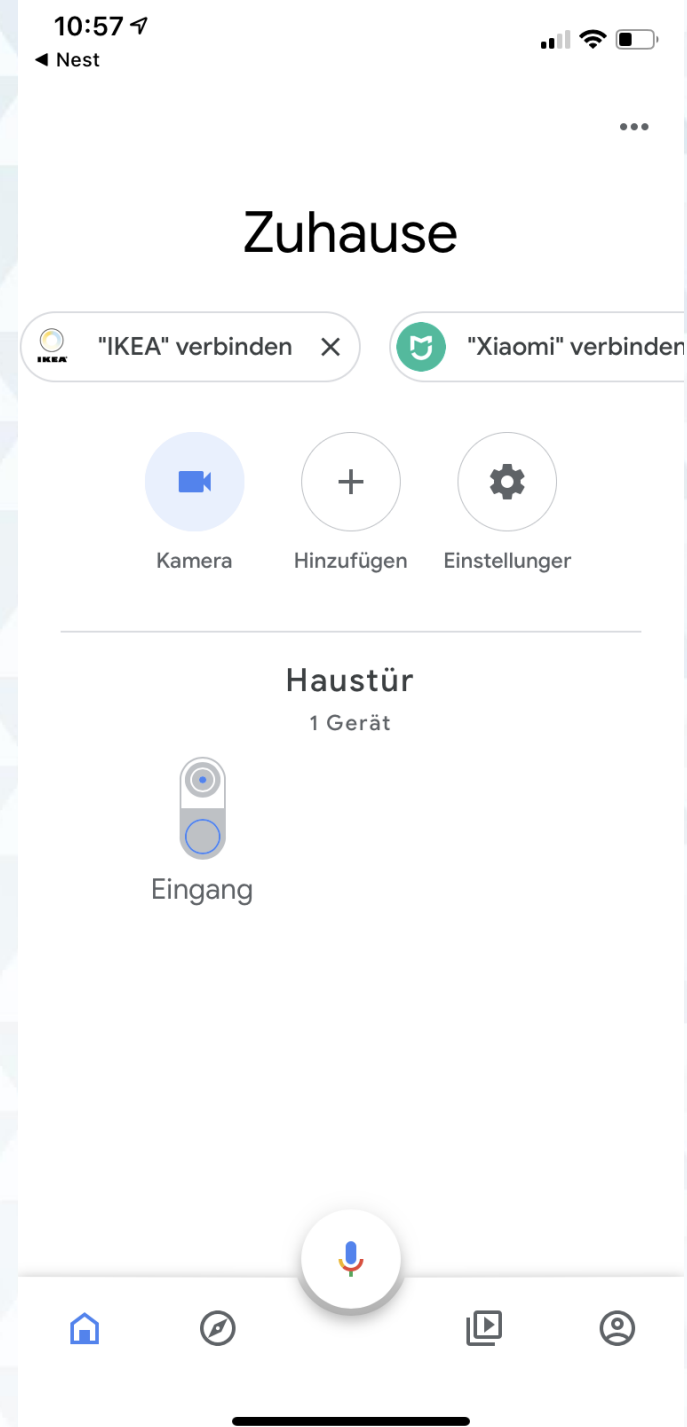
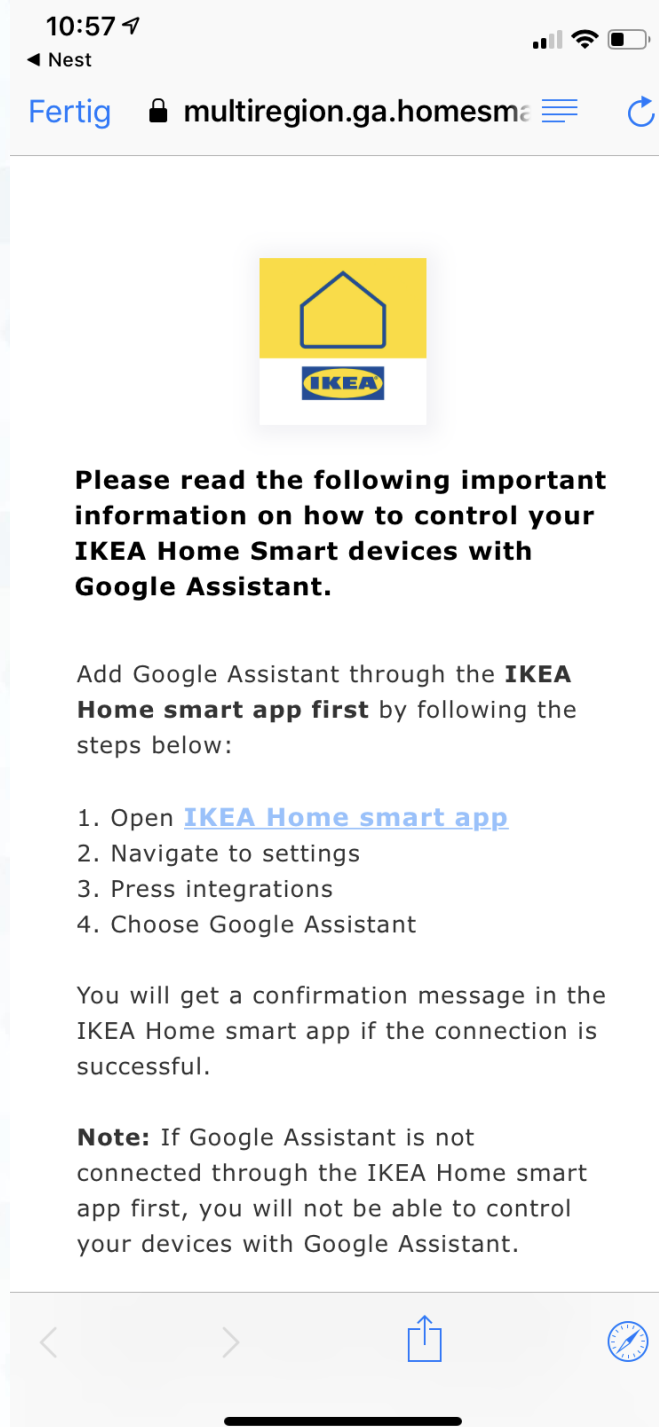
Login: admin
Password: admin

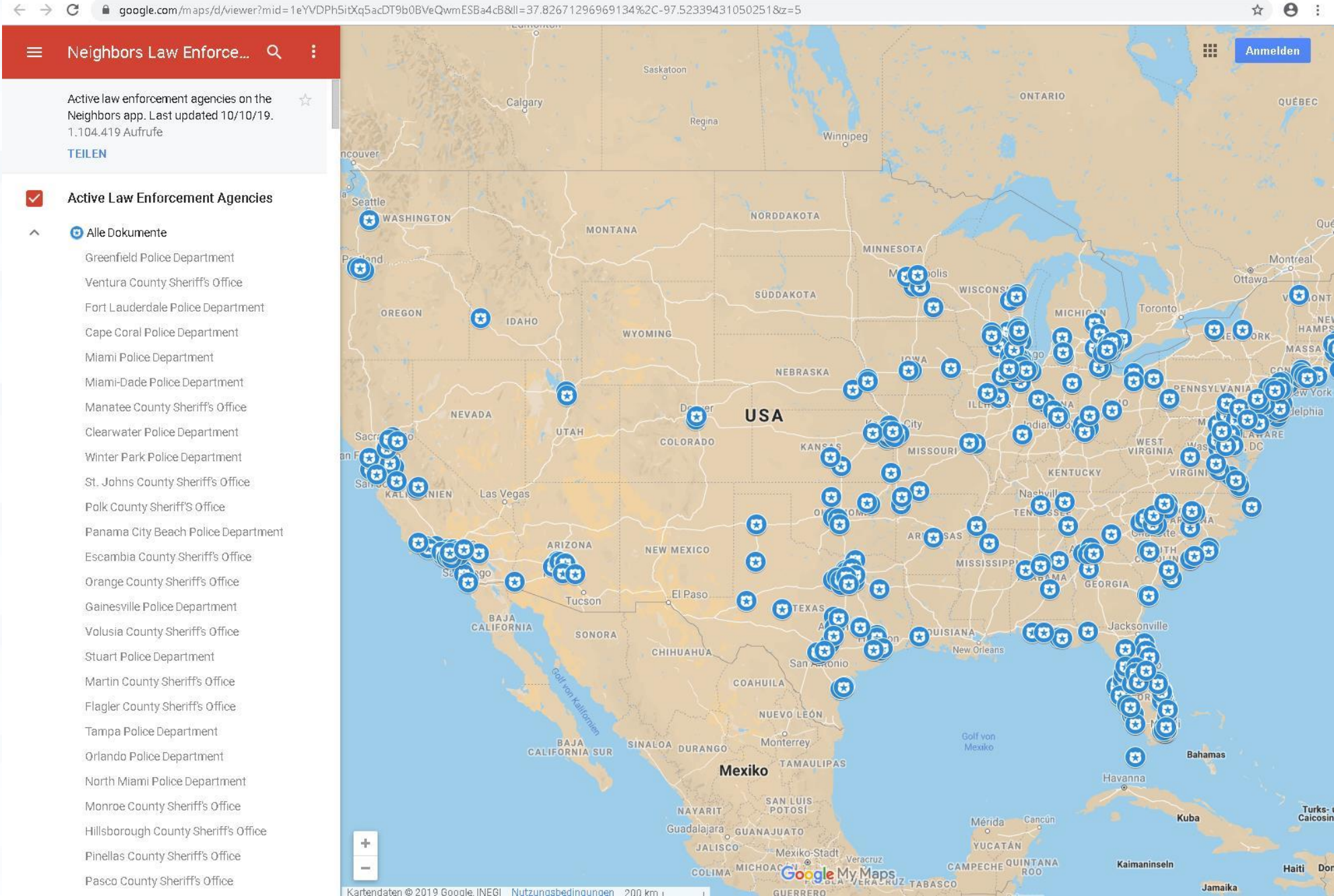


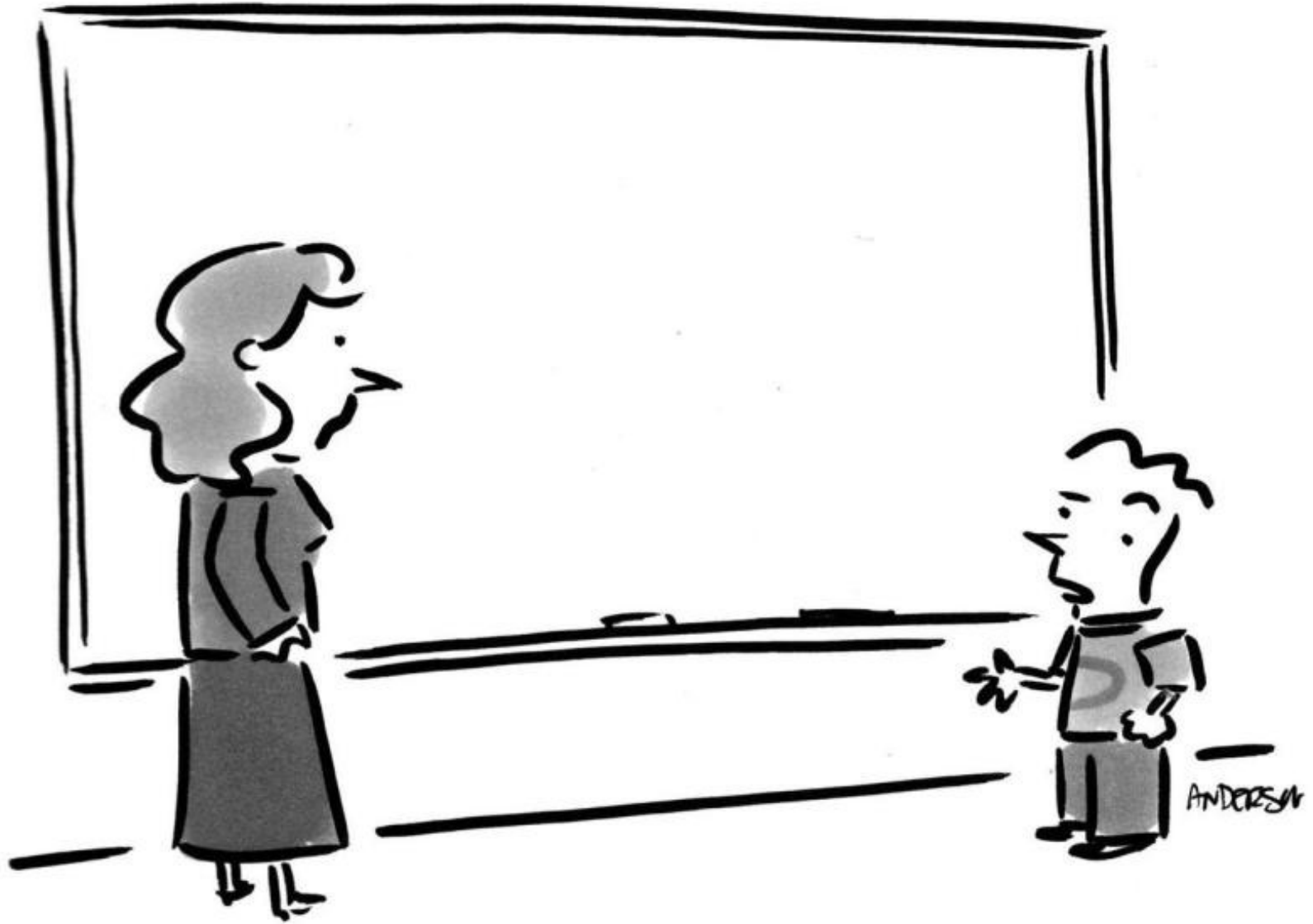


- Schutz der personenbezogenen Nutzerdaten auf dem Übertragungsweg und in der Cloud
 - Sammlung personenbezogener Nutzerdaten
-
- Immer noch häufig sträflich behandelt
 - Häufigste Probleme im Bereich der Datenschutzerklärung und ihrer Konformität zur **DSGVO**
 - Exzessive oder zumindest **unnötige Datensammlung** in vielen Fällen
 - Unzureichende Absicherung des Zugangs zu personenbezogenen Daten









"Before I write my name on the board, I'll need to know how you're planning to use that data."

Verfügbarkeit

- **Kritischer Sicherheitsaspekt** für Smart Home **Schutz- und Überwachungsanwendungen**
- Nur **schwerlich / nicht abzusichern**
 - Funkstörungen (Jamming)
 - Vor Ort immer möglich
 - Cloud-Anbindung
 - Ausfall des eigenen Anschlusses oder Cloud-Ausfall
 - Sensorausfall
 - Zerstörung / Defekt / Energieverlust

→ **Detektion und Meldung**



Netatmo @netatmo · 14. Nov.

Every room doesn't need to be heated the same way. We help you know what the ideal temperature in each room of your house is bit.ly/RoomTemperature

Tweet übersetzen



Kiran vadgama
@kiran_vadgama

@netatmo hi my manual override on my thermostat is not working and when i try using the app it comes up with an error with servers down. Can i override at boiler end?

2,2 Tsd.



Heikki Eräjorma @WhyDoYouAskThis · 23. Nov.

Antwort an @skoops @netatmo @internetofshit

The idiots who bought this trash deserve all the pain they're getting. Anyone who thinks that offloading ANY essential function to non-local server is a good idea should be shot outright and removed from the gene pool.

Tweet übersetzen





The Independent IT-Security Institute

Magdeburg Germany



AVTEST

The Independent IT-Security Institute

Magdeburg Germany



TESTURTEIL
» Sicher «

**GEPRÜFTES
SMART HOME
PRODUKT**



Vielen Dank für Ihr Interesse!



@avtestorg (English) & @avtestde (German)



Folgen Sie uns auf [facebook.com/avtestorg](https://www.facebook.com/avtestorg)

Aktuelle Testergebnisse auf <https://www.av-test.org>

