SMARTHOME DEUTSCHLAND

TeleTrusT
Pioneers in IT security.

IT-Sicherheit in smarten Gebäuden

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

Berlin, 29.10.2019

Smart Home Sicherheit –
Aus Sicht des Endkunden

Sven Boetcher,
Leiter Produktmanagement
eQ-3 AG

Smart Home – Bigger than ever?

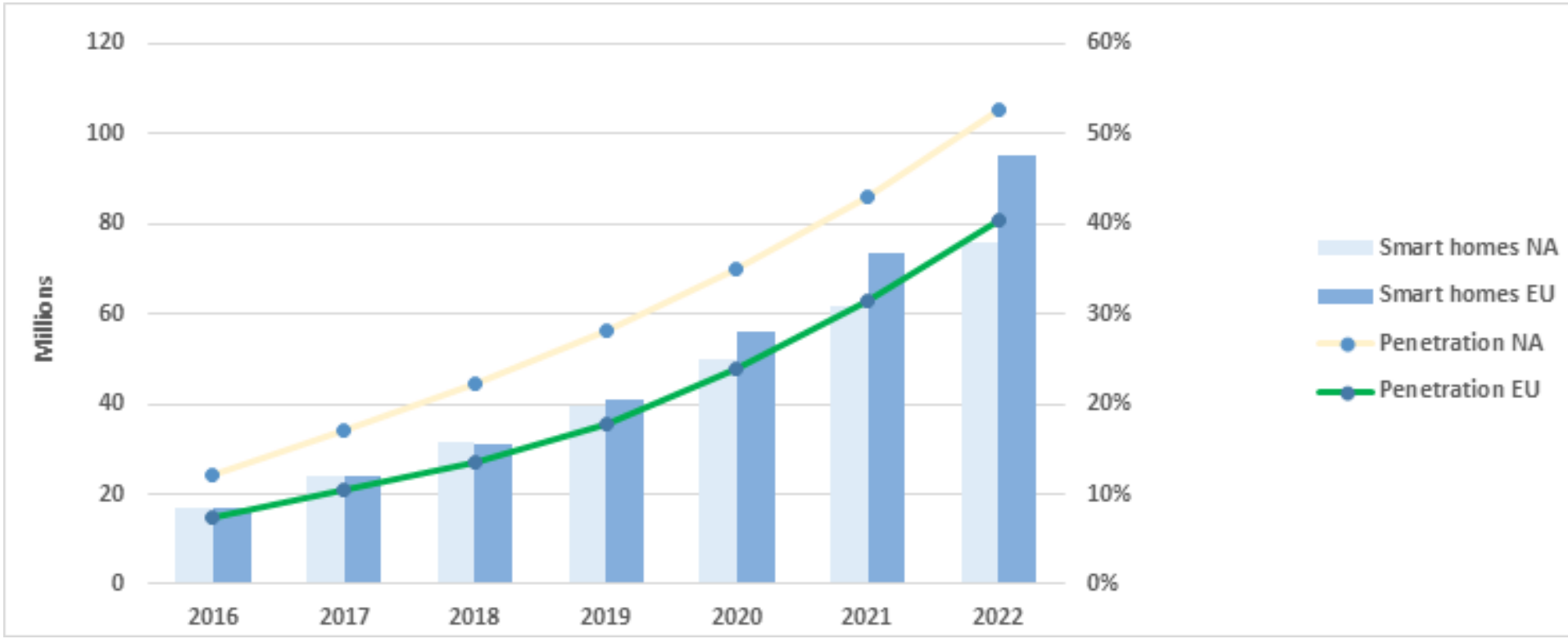
- Apple launches Homekit
- Google paid 3+ Billion USD for NEST
- RWE Smart Home is launched in Germany with large TV advertising – innogy restarts with Homematic IP
- Deutsche Telekom launched Qivicon
- Samsung launches SmartThings
- Amazon Alexa – Voice control for thousands of use cases including Home Control
- Google Assistant – Massive use of artificial intelligence for consumer use cases
- British Gas / Centrica “Hive” achieves over 250k customers in UK
- Bosch enters the Smart Home market
- eQ-3 sells over 33 million wireless devices to over 2 million households ➔ ***Homematic IP***

… or worse than ever?

- Consumers are interested in Smart Home, but get confused by the offerings
- Vendors do not respect and solve key concerns
- Large players spend on marketing, but don’t get traction
- Hive lost £ 2,05 for every £ 1,00 in revenue in 2017 (up from £ 1,54 in 2016)
- Home control systems and also Smart Home products are removed from shelves in CE retail…
- Products and their Cloud services are discontinued and customers feel like being left out in the cold…
- Most Home Control offerings simply fail in the market

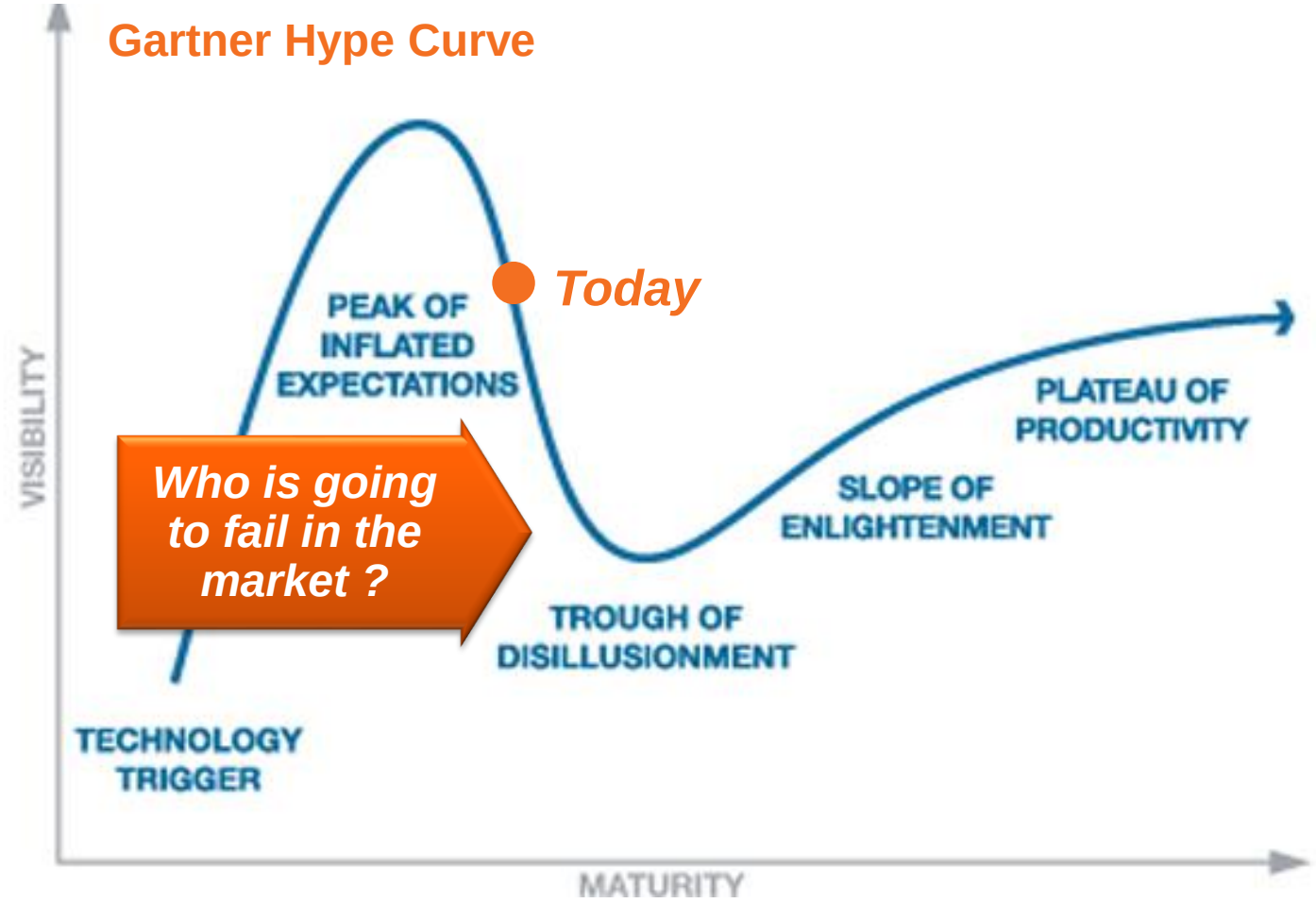
Smart Home Marktentwicklung?

Whole Home Systeme plus Punktlösungen



Source: Berg Insight, 2018

➔ ***What happened to the "50% of households in 5 years" predicted in 2012 by Analysts and Deutsche Telekom?***

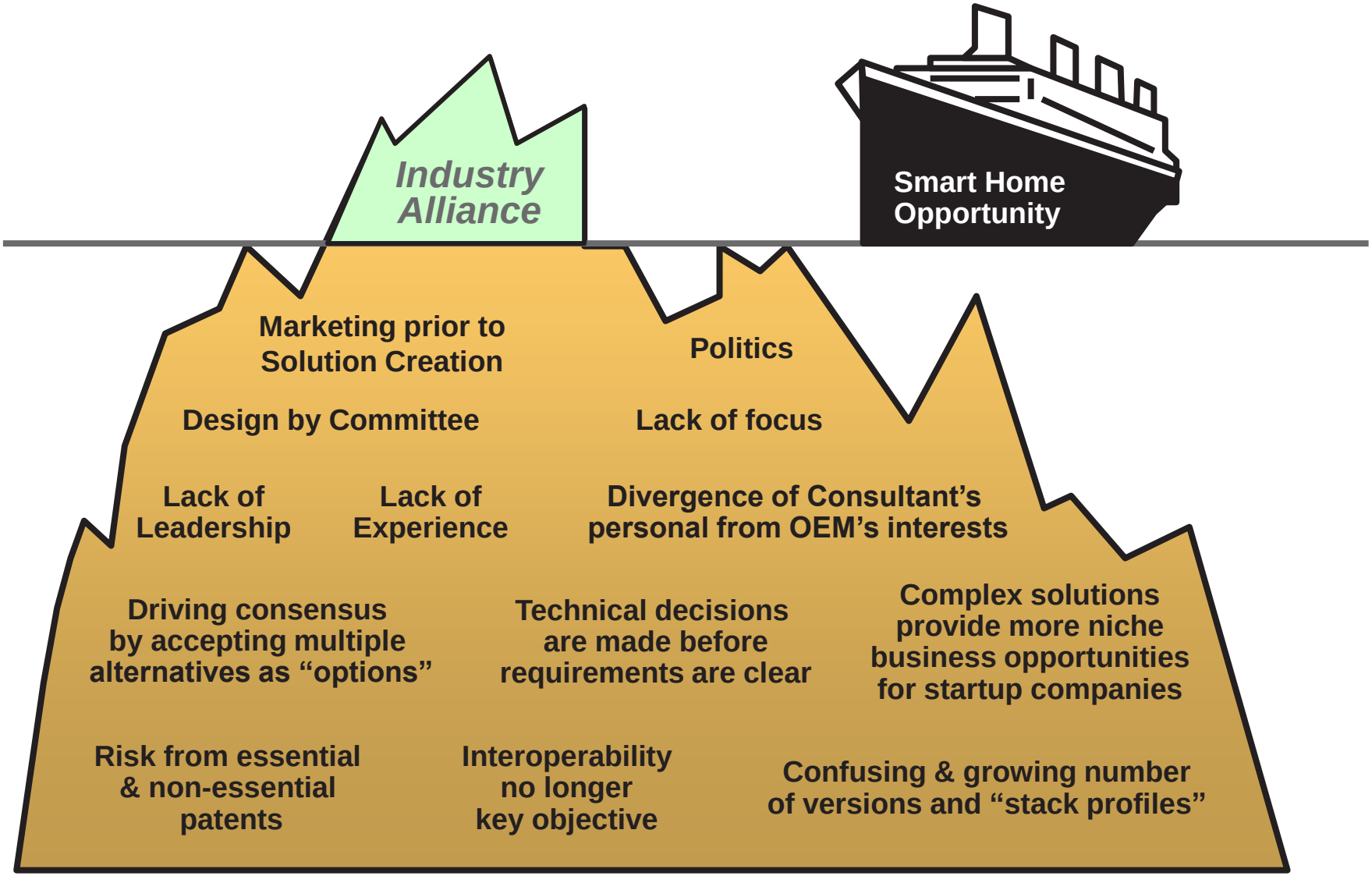


Source: Gartner Group

Problem: uns fehlt ein einheitlicher Standard

Dann gründen wir eine Industrie-Allianz und entwickeln den Smart Home Standard….

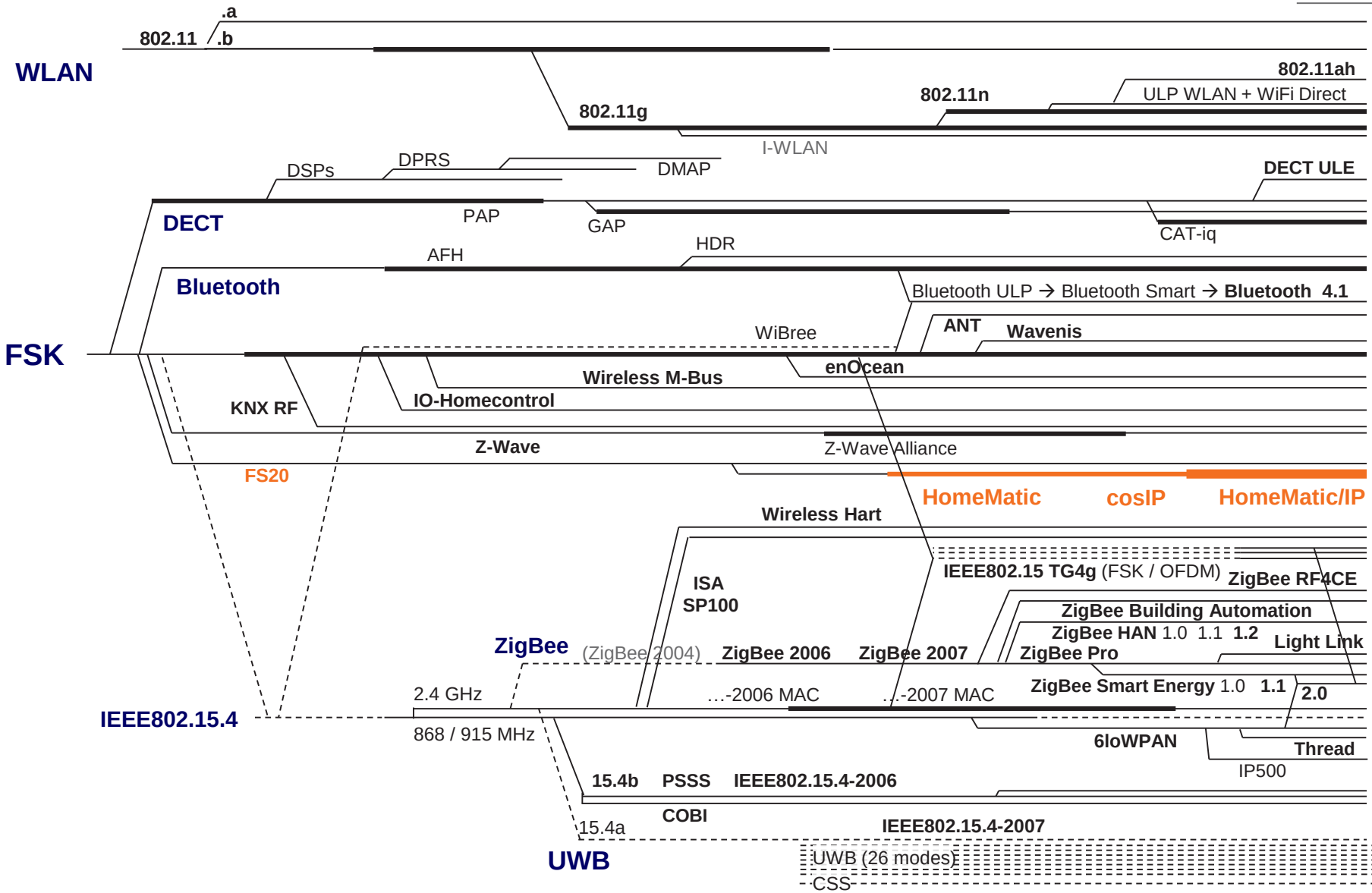
ILLUSTRATIVE



Dann gründen wir eine Industrie-Allianz und entwickeln den Smart Home Standard….

Die Anzahl von Smart Home "Standards" ist schneller gewachsen, als der Markt

ILLUSTRATIVE



bitkom

BITKOM Studie 2018	
37 %	empfinden die Installation der Technik als zu aufwendig
36 %	geben an, dass die Geräte zu teuer seien
33 %	hält die Bedienung für zu kompliziert
27 %	halten ihren Nutzen für zu gering
26 %	fürchten Hacker-Angriffe
24 %	haben Angst um ihre Privatsphäre
GFU Studie 2018	
65%	der Studienteilnehmer haben Sorgen in Bezug auf Datensicherheit und Datenweitergabe wegen der zunehmenden Vernetzung

bitkom

BITKOM Studie 2018		
37 %	empfinden die Installation der Technik als zu aufwendig	
36 %	geben an, dass die Geräte zu teuer seien	
33 %	hält die Bedienung für zu kompliziert	
27 %	halten ihren Nutzen für zu gering	
26 %	**fürchten Hacker-Angriffe**	➔ ***Cyber Security***
24 %	**haben Angst um ihre Privatsphäre**	➔ ***Cyber Security + Datenschutz***
GFU Studie 2018		
65%	der Studienteilnehmer haben Sorgen in Bezug auf Datensicherheit und Datenweitergabe wegen der zunehmenden Vernetzung	

➔ **IT-Sicherheit ist für uns doch heute gar kein Problem mehr....**

➔ **3 typische Beispiele, die über einfache IT-Sicherheit hinausgehen:**

WLAN in IoT / Smart Home Geräten

- Bei der Installation von IoT / Smart Home Geräten mit WLAN
  - müssen diese in das heimische WLAN integriert werden,
  - dafür muss das WLAN Passwort in das IoT Gerät....
- Das WLAN Passwort kann bei vielen (den meisten?) heutigen IoT-Geräten leicht abgehört werden
  - „*Das ist doch kein Problem: Wer weiss denn schon, wann ich anlerne?*...“ – Problem gelöst ???
- Gefahr von DoS + Social Engineering wird meistens übersehen:
  - Kommunikation mit dem IoT-Gerät wird gezielt gestört
  - Kunde wird typisch Support anrufen → und Hinweise / Anweisung zur Neuinstallation bekommen
- Beim folgenden Anlernen kann das WLAN Passwort einfach gestohlen werden
  - Die Gefahr liegt aber gar nicht primär beim IoT-Gerät / Smart Home
- ***Durch schlechte Security in WLAN-Geräten werden ALLE Geräte im Haus incl. Router angreifbar***
  - Identitätsdiebstahl + Angriffe auf Router (Revenue-Sharing bei Karibik-Telefonaten) sind REALE Risiken

Home Control 1 – „Standard A“

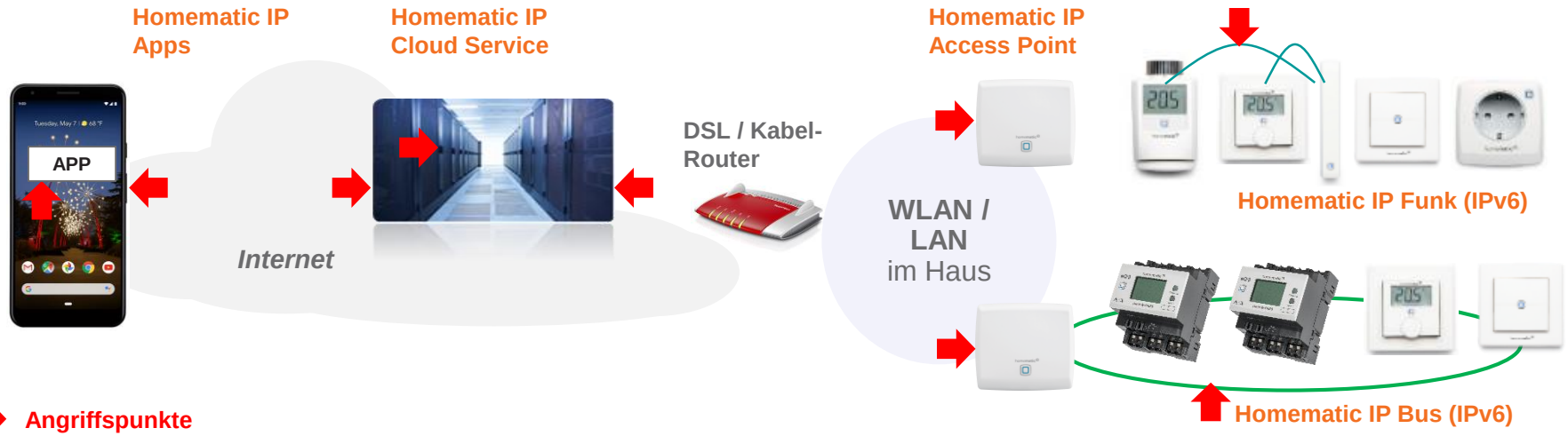
- Das Passwort für das Anlernen steht im Standard.... Und das Risiko wird wie bei WLAN unterschätzt
- ***Das entsprechende Netz ist für Angreifer offen für beliebige Manipulationen (z.B. mit Türschloss, Garagentor,.....)***

Home Control 2 – „Standard B“

- Anlernen wird mit einem modernen Verfahren mit asymmetrischer Ellyptic Curve Cryptographie geschützt
  - Und wir vertrauen alle, dass die NSA kein Verfahren gefunden hat, um....
- Beim Mesh Networking gibt es aber Probleme – Beispiel:
  Wenn man etwa 50x ein konstruiertes, ungesichertes Paket sendet (dauert etwa 10s, geht mit FSK Protoyp Board von Amazon), dann beschäftigt sich das Smart Home so sehr mit sich, dass reproduzierbar (!) >20 Minuten keine Nachrichten möglich sind
- ***Das entsprechende Smart Home erkennt für >20 Minuten kein Signal vom Fensterkontakt und löst keinen Alarm aus (!)***

- ***DAS WICHTIGSTE ZUERST: WIR MÜSSEN SICHERE LÖSUNGEN LIEFERN !!!***
  - Smart Home „Standards" helfen dabei offenbar eher nicht
- ***Technische Erklärungen und Akronyme? z.B. AES-128, RSA, Diffie-Hellmann, ECC, CCM...***
  - Werden von Endkunden nicht verstanden und **erhöhen** eher die Unsicherheit (!)
- **Zertifizierung**
  - ist eine weitaus bessere Lösung, den Endkunden zu überzeugen,
  - bestätigt und sichert durch Tests auch die tatsächliche Security der Smart Home Lösung,
  - muss dazu aber alle relevanten Aspekte der Cyber-Security abdecken,
  - regelmäßig widerholt und bezüglich Bedrohungen aktualisiert werden und
  - muss von einem international anerkannten Prüflabor mit 1A-Reputation stammen (!)
- eQ-3 hat sich daher für die Zusammenarbeit mit der VDE-Prüfinstitut entschieden.
- Homematic IP ist seit nunmehr 3 Jahren die **einzige Smart Home Lösung** mit **Zertifizierung der Protokoll-, IT- und Datensicherheit durch den VDE**

VDE
09/2018
Smart Home
Informationssicherheit geprüft
Homematic IP
www.VDEinfo.com
ID. 40046786



Die Homematic IP Cloud wird komplett anonym betrieben

bitkom

BITKOM Studie 2018		**Homematic IP**	
37 %	empfinden die Installation der Technik als zu aufwendig	✓	Die Stiftung Warentest hat im Jan. 2017 „bedienerfreundlich“ als Titel verwendet
36 %	geben an, dass die Geräte zu teuer seien	✓	Starterkits unter 100 Euro Heizkörperthermostatte für 29... 69 Euro „Smart Home jetzt auch ohne Aufpreis“
33 %	hält die Bedienung für zu kompliziert	✓	Stiftung Warentest, siehe oben
27 %	halten ihren Nutzen für zu gering	✓	Ersparnis: 30% Energie + 15...25 Mt CO2
26 %	fürchten Hacker-Angriffe	✓	VDE zertifizierte Protokoll-, IT- und Datensicherheit von Funk- und Bus
24 %	haben Angst um ihre Privatsphäre	✓	Anonymer Betrieb der Cloud
GFU Studie 2018			
65%	der Studienteilnehmer haben Sorgen in Bezug auf Datensicherheit und Datenweitergabe wegen der zunehmenden Vernetzung	✓	Siehe oben

Smart Home Standard?

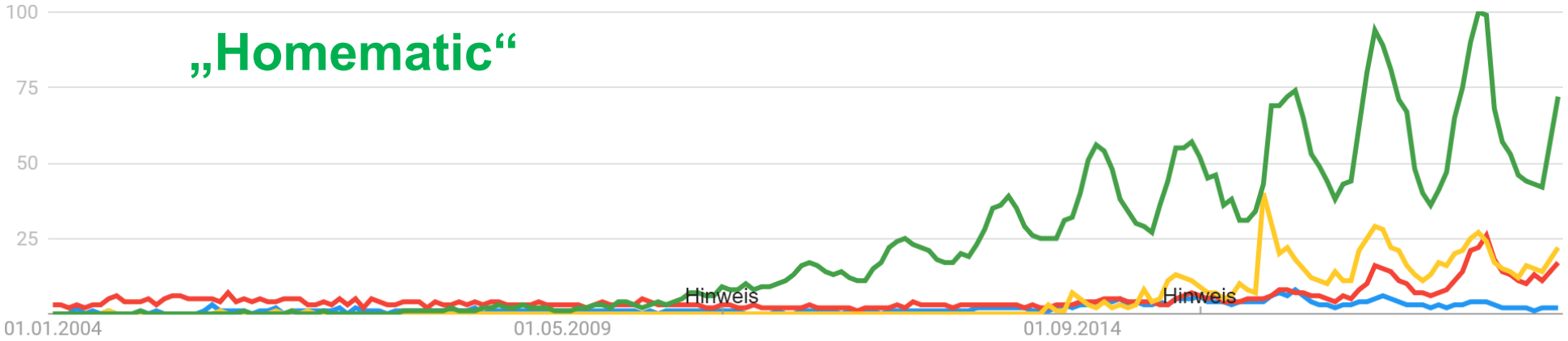
Google Trends: Die Sorgen und Wünsche der Endanwender ernst zu nehmen zahlt sich aus....

„Z-Wave“

„ZigBee“

„Homekit“

„Homematic“



Germany – 22-October 2019

Berg Insight: Smart Homes and Home Automation

eQ-3 ist der europäische Marktführer[1]

Company name		Berg Insight 2017 EOY 2016	2018 EOY 2017	Year-to-Year Growth
eQ-3	**HM + Homematic IP**	387.000	**670,000**	**81%**
eQ-3 incl. OEMs [3]		600.000	**980.000**	**63%**
Deutsche Telekom	Qivicion	150.000	280.000	
Verisure	Monitored security	250.000	260.000	
Somfy	Windows controls	(in others)	140.000	
RWE / innogy	Energy company	75.000	100.000	
KNX systems [2]		80.000	80.000	
Loxone		55.000	65.000	
Others	Home control systems	403.000	700.000	
Total		**1.400.000**	**2.300.000**	**64%**

TODAY

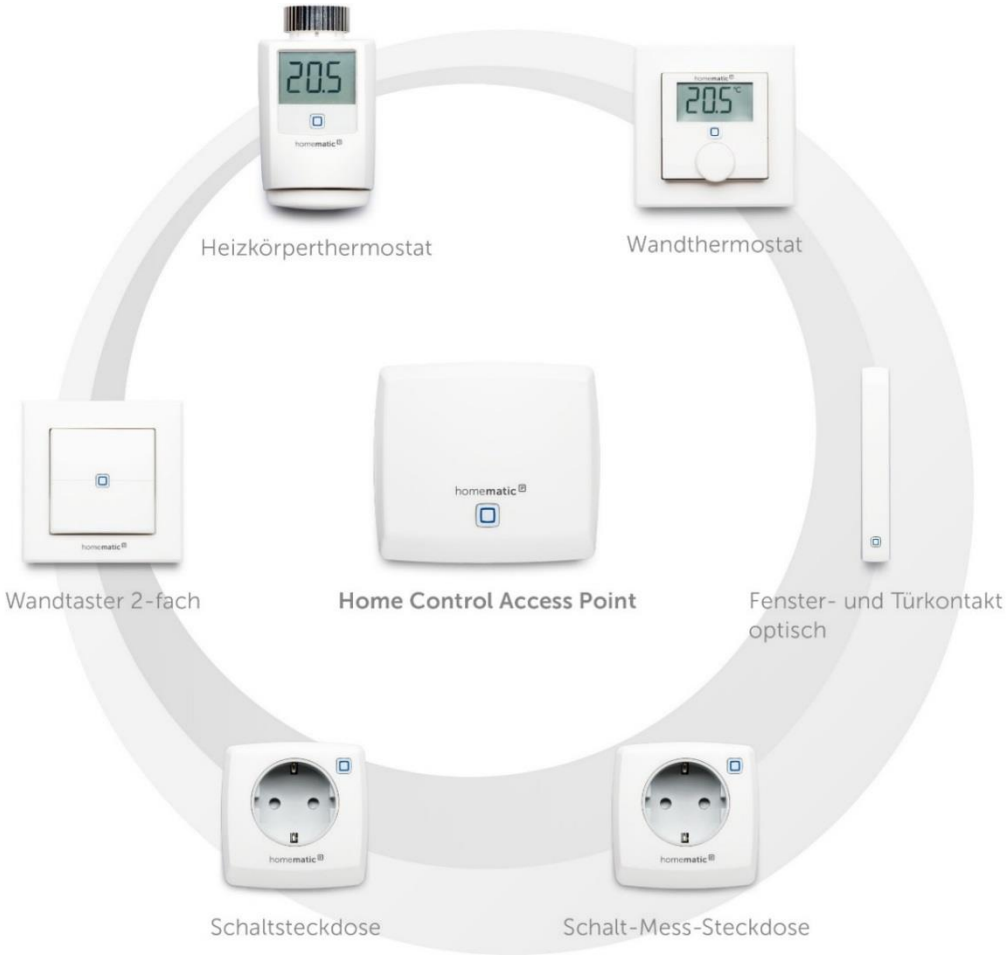
Over 2.000.000 households with eQ-3 home control solutions[3]

More than 33 million wireless Smart Home devices from eQ-3

1: Whole Home Solutions (installed base); 61% if counting all wireless home control solutions from eQ-3 (Berg Insight, September 2018)
2: ABB, Hager, Schneider Electric, Gira, Jung and several other vendors
3: Including other product lines such as MAX!

Warum ist Homematic IP bei Endkunden so erfolgreich?

Smartes Wohnen, einfach begeisternd **–** *Homematic IP stellt den Anwender an die erste Stelle*



Over 90 types of devices already available today

- **Easy to install, configure, use (!)**
  - Stiftung Warentest: “Easy to Use”
- **Robust + reliable:**
  Builds on the Strength of Homematic, e.g.
  - 868 MHz frequency band
    → No interference from high speed WLAN
    → Best range and robustness
  - HomeMatic application protocol
    → Proven in millions of devices
  - Strength in battery-to-battery operation
  - Homematic IP and Homematic are COMPATIBLE
- **Best-in-Class security**
  - Authentication + encryption of all messages
  - Cryptographically secure device installation
  - VDE Security Certification of Protocol, IT, and data
- **Best in Class Data Privacy**
  - Anonymous cloud operation is ideal for consumers
- **According to Stiftung Warentest the only solution with commitment to long-term availability**
  - Binding commitment at least until the end of 2030 [1]
- **Lowest entry cost thanks to Home Access Point**
  - Like in WLAN access points, no SW updates are required for new / changed device
- **IPv6 in all devices**
  - Convincing position towards standardization
- **Homematic IP is OPEN**
  - Linux based SW for Central Unit free on GitHub
  - APIs and libraries openly available
  - Technology licenses have already yielded multiple independent stack implementations

Danke !