

# **IoT-Sicherheit: Was ist neu und was wichtig?**

Prof. Dr. Steffen Wendzel  
Hochschule Worms / Fraunhofer FKIE

<http://www.wendzel.de>

Steigende Komplexität und gegenseitige Abhängigkeit vernetzter IoT-Systeme.

# KOMPLEXITÄT

>>> Beispiel: Historie der Gebäudeautomation.

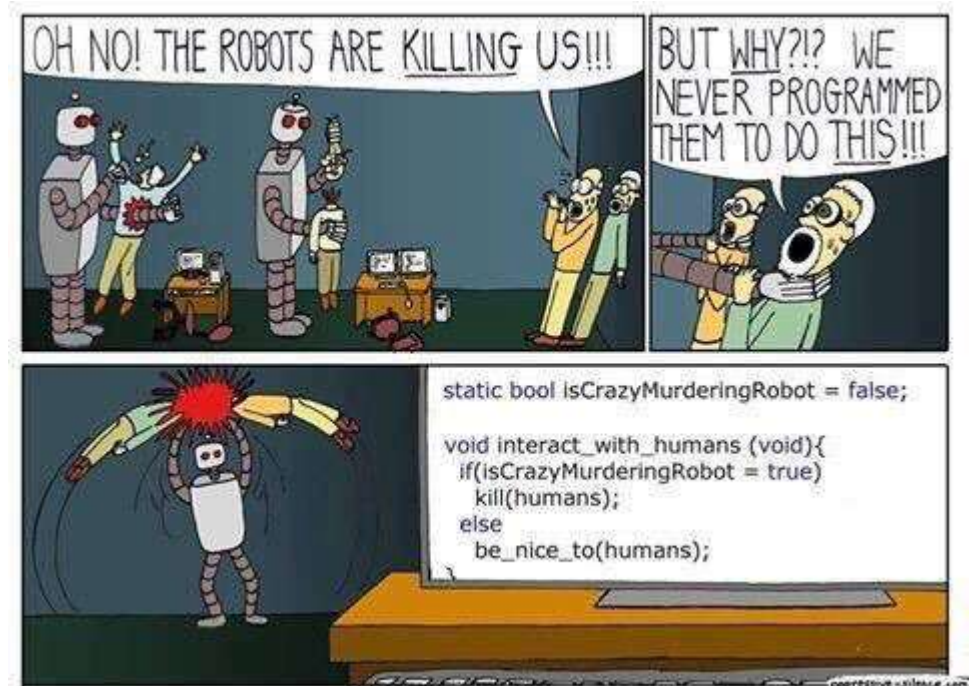
Wie sieht es aus mit der

# VERANTWORTUNG DER HERSTELLER?

>>> Verantwortung beim klassischen Automobil?

Quelle: Leverett et al.: Standardization and Certification in the 'Internet of Things', in Proc. WEIS, 2017.

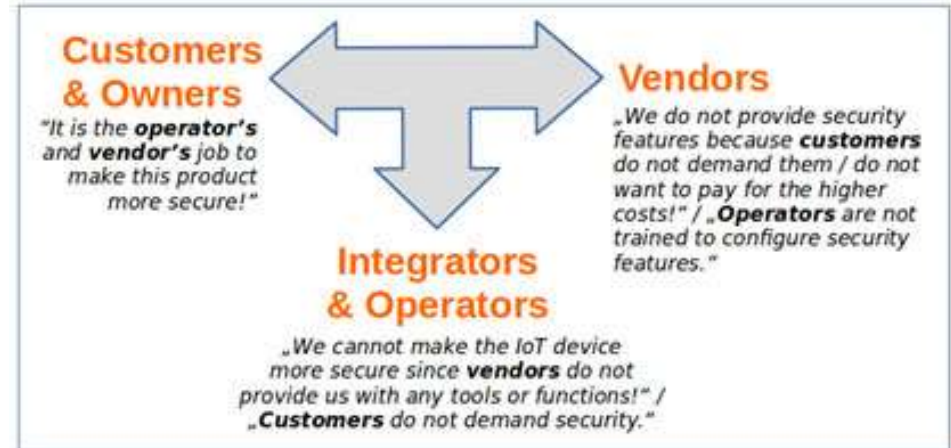
- IT-Sicherheit ist nur mit viel Aufwand für den Hersteller überprüfbar.
- Kunden und Staat können diese Überprüfung nur begrenzt übernehmen, jedoch **Verantwortung fordern**.



- Ein Grundproblem ist die Sichtweise des „sicheren IoT-Produkts“, denn:
  - Attribut „sicher“ gilt nur für den Zeitpunkt der Überprüfung (und für den Umfang dieser Überprüfung).



- Schuld ist immer ein anderer Beteiligter.
- Modell im Wesentlichen anwendbar auf alle IoT-Domänen.
- Wie CoB beenden?
  - Sicherheit als Marktvorteil (ähnlich „Made in Germany“) betrachten
  - Druck auf Hersteller ausüben
- Lösungen sichtbar, etwa bei Smart Buildings.  
Große Verbesserungen binnen weniger Jahre erzielt!



## IT-Sicherheitskongress: BSI-Chef befürwortet neue Haftungsregeln

 heise online 17.05.2017 15:26 Uhr - Torsten Kleinz

 vorlesen

### Cyber-CE-Siegel

Um das Dilemma zu lösen, müsse der Staat eingreifen. So plädierte Schmidt dafür, Hersteller für die Schäden durch ihre Produkte haften zu lassen. Ein geeignetes Mittel könne ein Sicherheits-Siegel ähnlich dem CE-Siegel sein, mit dem Hersteller garantieren, wesentliche Sicherheitsstandards einzuhalten und Updates für eine gewisse Geräte-Lebensdauer zu liefern.

Arne Schönbohm, Chef des Bundesamtes für Sicherheit in der Informationstechnik, erklärte daraufhin: "Ich bestärke die Politik, den Weg zu gehen, den Sie gerade geschildert haben." Allerdings sei seine Behörde nur mit der Umsetzung der Gesetze beauftragt und könne keine eigenen Regeln aufstellen.

[Linkschleuder](#)

## **Internet der Dinge: Hersteller deaktiviert Garagentoröffner nach schlechter Kundenbewertung**

am 07.04.2017 von David Richter / 6 Kommentare / Teilen







- ... haben in der Regel viel Zeit, um IoT-Equipment anzugreifen.
- ... kennen die Sicherheitstechniken von Produkten (bzw. bringen diese in Erfahrung).
- Neue Produkte bieten ständig neue Funktionen, die potenziell angegriffen werden können.



- Wenig Speicher
- Geringere Rechenleistung, insb. bei Smart Objects
- Begrenzte Batterielaufzeit
- Permanente Verfügbarkeit erwartet (etwa permanentes Messen von Sensorwerten oder permanentes Steuern des Drucks in einem Behälter)
- Teils proprietäre Protokolle

- Dadurch ergeben sich einige **Besonderheiten**:
  - JIT-Handling von rechenintensiver Kryptographie nur begrenzt möglich
    - Ressourcen-effiziente Kryptographie vorteilhaft
    - Insbesondere für altes Equipment (-> heute+20y/+30y)
  - Kunden erwarten Kombination:  
langer Laufzeit von IoT-Equipment + IT-Sicherheit
  - Upgrades werden u.U. schwierig
    - Restarts beeinflussen kurzzeitig die Verfügbarkeit
    - IoT-Equipment muss nach einem Upgrade evtl. neu zertifiziert werden
    - Nicht alle Things sind leicht erreichbar (evtl. in physikalisch geschlossenem System verbaut oder an abgelegenen Ort/Wildtier platziert)
  - Sicherheitsscans müssen diverse (proprietäre) Protokolle abdecken

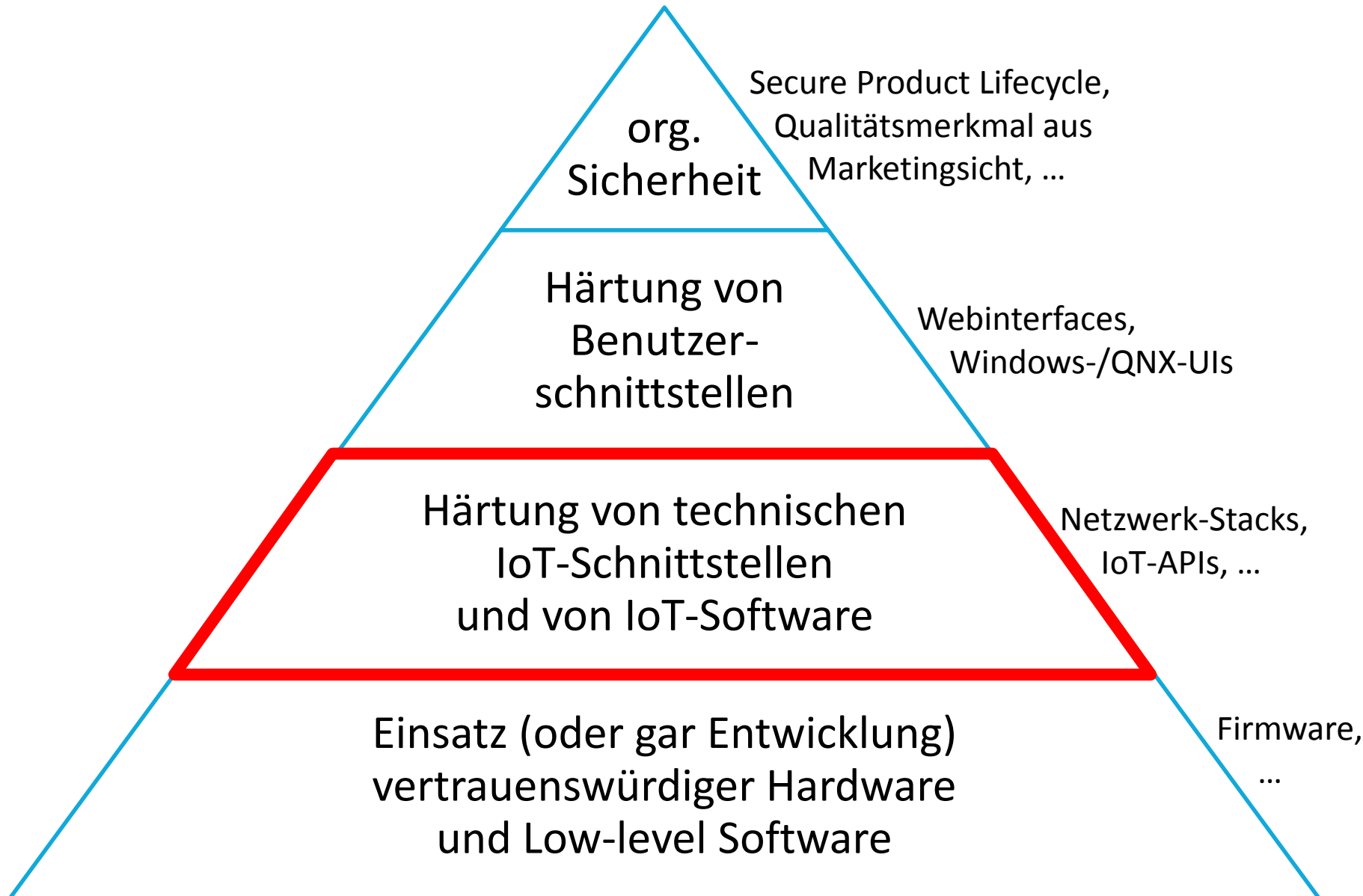
- IoT-Botnetze können prinzipiell sämtliche Arten von IoT-Geräten beinhalten.
- Standardszenarien:
  - Versenden von Spam
  - Durchführung von DDoS-Angriffen
- Andere Szenarien: Ausnutzung physikalischer Fähigkeiten (beeinflusst **nicht nur Security**, sondern **auch Safety**):
  - Szenario Smart Building Botnets
  - Energieverbrauch einer Smart City/Area erhöhen -> mehr Absatz für Öllieferanten
  - Überwachen von Bewohnern, Kunden, Personal, ...
  - Planen von Einbrüchen
  - (D)PDoS (*Distr. Permanent DoS*), etwa Kaputtmachen aller Smart Cars eines Herstellers durch die Konkurrenz oder aller Überwachungskameras einer Region bevor dort ein terroristischer Anschlag durchgeführt wird.



- tech./org. Hürden
- Auswirkung auf Daten, die die physikal. Umwelt beschreiben (nicht-IT-Forensik)

Property	Relation to (digital) forensic investigation	Exemplary challenges
Density of device deployment	Influences the resolution of events that took place in a physical environment.	Reconstruct physical events on the basis of unevenly deployed devices (for example, not all the space has the same density of Internet of Things [IoT] nodes and information). This can also vary according to the considered environment.
Device type	Influences the type of information (sensor data such as temperature, humidity, pressure, or motion detection as well as the history of actuator states such as door status, pump pressure, or heating level).	Provision of a computer-aided, evidence-driven, and court-proof framework for the reconstruction of events. Such software should be able to take into account a mixed/increasing set of devices, for instance by means of a plug-in architecture.
Device location	Influences physical accessibility of the device for a digital forensic investigation (the device might be placed behind country borders) and influences which area of a physical environment was covered by the device (the part of a forensic site that has been influenced).	Develop a cost-benefit analysis to determine whether IoT devices located in hard-to-reach areas are worth accessing. One idea is to use databases that point out device properties useful for forensics investigations and additional details such as the accuracy of onboard sensors.
Recording history	All available information on an IoT device can be recorded locally or in the cloud. Local storage is usually limited; thus, the number of recorded sensor values/actuator states is kept under a certain threshold. Older data might not be accessible.	Automatic integration of IoT devices into the reconstruction process of physical events. This requires fetching the recording history of sensors and correctly placing it within the time frame of the event to be reconstructed. It could entail the support of visual analytics tools capable of handling devices that provide data with inconsistent or inaccurate timing and spatial positions.
Device interfaces	The interfaces used to access evidence highly influence the amount of information that can be retrieved. Some types of information might not be provided by certain interfaces while others are. In several cases, interfaces might be undocumented by the vendor.	Provision of a unified metainterface for IoT forensics covering a large spectrum of different devices and low-level interfaces of several vendors. This can likely be adequately addressed by larger community projects.

Quelle:  
L. Caviglione, S. Wendzel,  
W. Mazurczyk: [The Future of Digital Forensics: Challenges and the Road Ahead](#), in: IEEE Security & Privacy Magazine, Nov/Dez 2017.



- Forschungsprojekt **BARNI**
  - Förderung durch BMBF (2014-2016)
  - Fraunhofer FKIE, Bonn + MBS GmbH, Krefeld



- **Arbeitsgebiete:**
  - Traffic Normalization
  - Traffic Analysis
  - Visual Analytics



# BARNI Normalizer

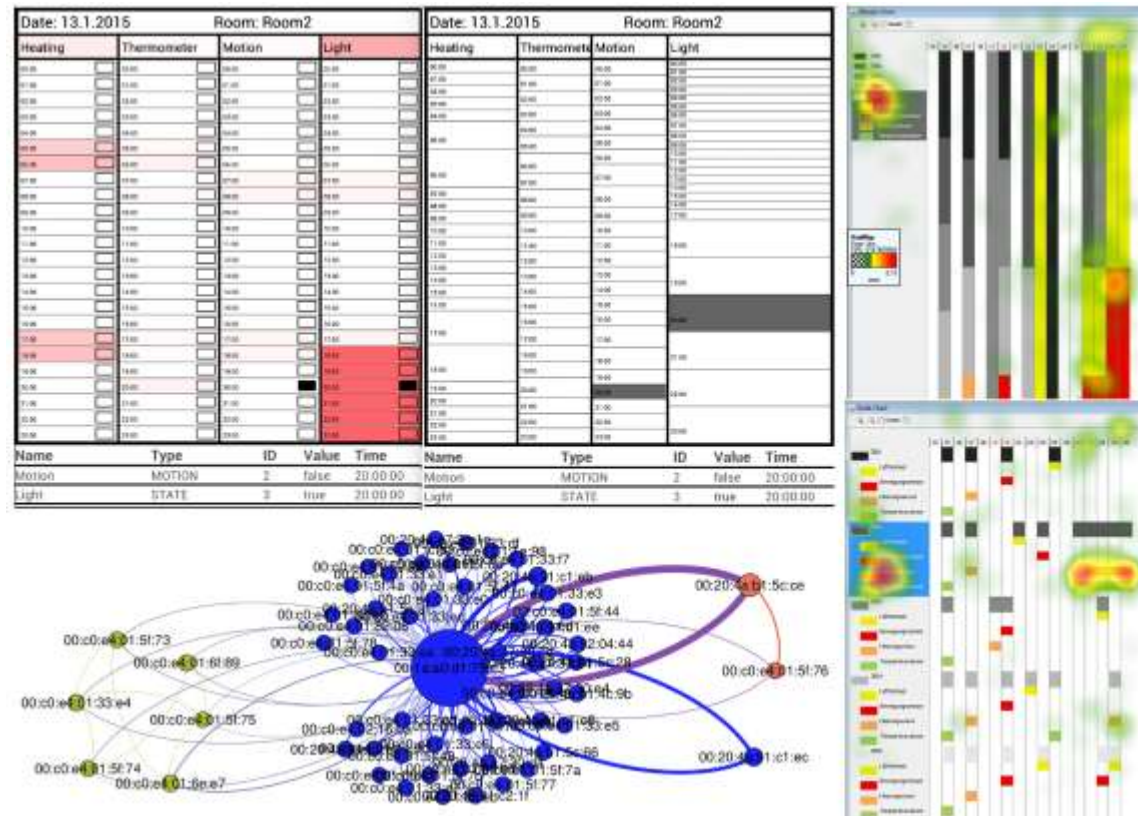


Visualisierung von Anomalien für verschiedene **Gerätetypen:**

- Operator Workstations
- Smartphones

Anomalieerkennung auf verschiedenen **Ebenen:**

- Datenverkehr im Netzwerk
- Sensorwerte und Aktorzustände



## Traffic Normalization:

Abschottung von potenziell verwundbaren Geräten durch Entfernen potenziell schädlicher Elemente aus dem Datenverkehr.

- Traffic Normalization kann für alle Netzwerkprotokolle eingesetzt werden.
- Kann Nachrüstungsproblematik eindämmen.
- Somit anwendbar für noch unbekannte Angriffe und Langzeit-Deployment von IoT-Equipment (grundlegende Probleme des IoT).

## Beispiel:

- Ein unsicherer Netzwerkstack sei nur mit hohem Aufwand patchbar.
- Traffic Normalization schottet den Netzwerkstack ab (entweder integriert in Produkt oder als separater nachrüstbarer Gateway).

Quellen:  
S. Wendzel: [How to Increase the Security of Smart Buildings](#), in: Communications of the ACM (CACM), Vol. 59(5), 2016.  
J. Kaur et al.: Securing BACnet's Pitfalls, in Proc. IFIP SEC, Springer, 2015.

- Die Herangehensweise, Produkte initial einmalig sicher zu gestalten und dann auf den Markt zu bringen, ist nicht genug.
  - Heute dem Stand der Sicherheit entsprechend, in einigen Jahren veraltet und nicht mehr nachrüstbar.
  - IT-Sicherheit wird für das Internet der Dinge aufwendig.
    - Smart Cars und Smart Buildings sind über Jahrzehnte im Einsatz!
- **Die Industrie sollte sich vom Internet der Dinge nicht abwenden.** Zu viele Chancen sind mit dem IoT verbunden.
- Bei der Entwicklung von IoT-Produkten sind **allerdings langfristige Lösungen gefragt.** Mögliche Wege sind zum Beispiel:
  - Traffic Normalization
  - KI zur Detektion bisher unbekannter Angriffe
  - Gemeinsame Forschung mit Hochschulen, Universitäten, Forschungseinrichtungen -> **kommen Sie gern auf mich zu.**

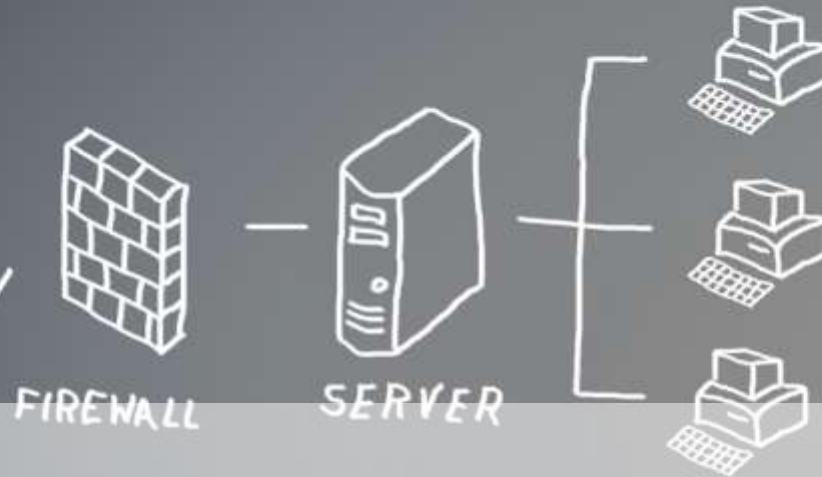
Quellen:

A. Kobekova: Was bedeutet das IT-Sicherheitsgesetz für Smart Buildings?, Tagungsband z. IT-Sicherheitskongress de BSI, 2017.

J. Kaur et al.: Securing BACnet's Pitfalls, in Proc. IFIP SEC, Springer, 2015.



Hochschule  
Worms  
University of Applied Sciences



**Vielen Dank für Ihre  
freundliche Aufmerksamkeit!**

**Kontakt:**

Prof. Dr. Steffen Wendzel  
wendzel@hs-worms.de