

# **17. Augsburger Linux-Infotag**

## **Das Internet der unsicheren Dinge**

**Talk by Barbara Wimmer**

Contact: [shroombab@gmail.com](mailto:shroombab@gmail.com)

Twitter: @shroombab

# Internet der Dinge

- **Warum beschäftige ich mich damit?**
- **Was bedeutet Vernetzung für die Gesellschaft?**
- **Was bedeutet es für unsere Privatsphäre?**
- **Und - was für Alternativen gibt es?**

13 Jahre lange Erfahrung als IT-Journalistin, schreibe über IT-Security, Datenschutz und Netzpolitik und verfolge alle möglichen „smarten Innovationen“ mit. 2014 habe ich mit dem österreichischen CERT zum ersten Mal darüber gesprochen, als der erste Kühlschrank Spam-E-Mails verschickt hatte.

# **Internet der Dinge**

## **Wearables:**

**Smart Watch, Fitness Tracker**

**Kinderspielzeug, Sexspielzeug**

**Alles rund um Heimvernetzung**

## **Digitale Assistenten**

**und smarte Lautsprecher:**

**Google Home mit Assistant, Amazon Echo mit Alexa, Apple Siri,  
Microsoft Cortana**

# Internet der Dinge

- **Wer von euch hat ein oder mehrere IoT Geräte zu Hause?**
- **Home Automation?**
- **Digitale Assistentin?**
- **Wie viele davon sind selbstgebaut und basieren auf Open Source?**

# Internet der Dinge

Category	2016	2017	2018	2020
Consumer	3,963.0*	5,244.3	7,035.3	12,863.0
Business (cross industry)	1,102.1	1,501.0	2,132,6	4,381,4
Business (vertical specific)	1,316.6	1,635.4	2,027.7	3,181.0
<b>Grand- Total</b>	<b>6,381,8</b>	<b>8,380.6</b>	<b>11,196,6</b>	<b>20,415.4</b>
Source: Gartner (January 2017)	*MILLIONS			

## Drei-Chef: "Vernetzung kann man nicht aufhalten"



von Barbara Wimmer 28.09.17, 08:00 [shroombab](#) [Mail an Autor](#)

**„Vernetzung wird überall dort entstehen, wo es einen wirklichen Nutzen für Kunden bringt. Das wird man auch nicht aufhalten können und wollen.“**

**Jan Trinow, Drei-Chef Österreich**

INTERNET DER DINGE

Max Schrems: "Wie viel Vernetzung ist eigentlich gesund?"



von Barbara Wimmer 09.09.17, 06:00 [shroombab](#) [Mail an Autor](#)

**„Bei jeder neuen Technologie gibt es erst einmal einen Wahn und alles wird gemacht, was geht. Wir müssen uns irgendwann aber die Frage stellen, wie viel Vernetzung eigentlich gesund ist.“**

**Max Schrems, Datenschutzaktivist**

# Max Schrems





# Smart Coffee Maker

- kann sich mit anderen Dingen vernetzen

Wie Fitness- und Schlaf-Tracker

- Nutzen: wenig Schlaf - starker Kaffee

- Gefahr: Wem gehören diese Daten?

Mit wem werden sie geteilt?

Wenn ich vom „Internet der unsicheren Dinge“ spreche, meine ich nicht nur IT-Security. Stellen wir uns mal vor, die Daten gelangen in die Hände einer Versicherung. Wenn jemand regelmäßig zu wenig schläft und zu starken Kaffee trinkt, steigt möglicherweise das Risiko für Burn Out oder Herzerkrankungen und die Versicherung wird teurer.

## Symbolbild / fiktives Beispiel



Oder was wäre eigentlich, wenn der Kaffeemaschinenhersteller pleite geht, weil es sich um ein hipbes Start-up gehandelt hat, dem plötzlich das Geld ausging? Da will ich jetzt von der hypothetischen Annahme zu einem echten, praktischen Beispiel kommen, das schön zeigt, dass Unsicherheit nicht nur durch IT-Security entsteht...

# Emberlight: echtes Beispiel

The screenshot shows a webpage from Network World with the following content:

- Header:** NETWORKWORLD
- Article Title:** What happens when an IoT implementation goes bad?
- Text:** The failure of Emberlight reminds us that Internet of Things devices may not work when the vendor stops supporting them.
- Image:** A photograph of the Emberlight smart light bulb, which is a standard incandescent bulb with a white base, sitting on a wooden block next to a small air plant.
- Related Articles:**
  - Real-world examples of IoT rolled out in the enterprise
  - IoT market keeps growing, with no end in sight
  - Review: Microsoft Azure IoT Suite
  - What's next in IoT innovation?

Das Start-up Emberlight hat im Jahr 2014 300.000 Dollar eingesammelt, um eine smarte Glühbirnenhalterung zu entwickeln, die mit gewöhnlichen Glühbirnen funktioniert. Im November 2017 gab Emberlight bekannt, dass es das Geschäft einstellt, weil größere Wettbewerber ihr Produkt kopiert hatten und es für ein Viertel des Preises anbieten.

# **Emberlight**

## **Problem:**

**Permanente Cloud-Verbindung zu den Servern notwendig**

## **Konsequenz:**

**Start-up weg, Lichter aus**

Doch was bedeutet das jetzt für die Kunden, die Emberlight-Halterungen gekauft hatten? Sie mussten alle ihre smarten Glühbirnenhalterungen nun wieder auswechseln, weil diese eine permanente Cloud-Verbindung verlangt hatten und Emberlight die Server abgedreht hatte. Ohne Server ging aber auch das Licht bei den Nutzern nicht mehr an oder aus.

## **Beachten:**

**Bei Start-ups kann es passieren,  
dass es unvorhergesehene  
Probleme gibt,  
an die zu Beginn  
keiner gedacht hat**

Doch was bedeutet das jetzt für die Kunden, die Emberlight-Halterungen gekauft hatten? Sie mussten alle ihre smarten Glühbirnenhalterungen nun wieder auswechseln, weil diese eine permanente Cloud-Verbindung verlangt hatten und Emberlight die Server abgedreht hatte. Ohne Server ging aber auch das Licht bei den Nutzern nicht mehr an oder aus.

## **Echtes Beispiel: IoT-Drosselung**

**In den USA drohte ein Internet-Provider seinen Kunden damit, dass auch vernetzte Thermostate und Überwachungskameras nicht mehr funktionieren würden, wenn er die Verbindung drosselt.**

Ein US-Internet-Service-Provider „Armstrong Zoom“, der an der Ostküste der USA rund eine Million Kunden hat, bedrohte seine Kunden, die beschuldigt werden, Urheberrechtsverletzungen begangen zu haben, mit dem Nicht-Funktionieren ihres Thermostats. Provider sind dort aufgrund der Aufhebung der Netzneutralitätsgesetze in der Lage, Internetverbindungen zu reduzieren.



An der Ostküste wurde aber prompt für das besagte Wochenende eine Eiseskälte mit Temperaturen weit unter 0 Grad vorhergesagt. Ein nicht funktionierender Thermostat könnte für manche der Bewohner daher durchaus lebensbedrohlich, oder zumindest stark gesundheitsgefährdend sein. Zudem kommt es öfters vor, dass Filesharing-Briefe routinemäßig an Unschuldige ausgestellt werden.

## Frage

**Darf ein Provider wirklich  
über Leben und Tod  
entscheiden, weil jemand  
„Game of Thrones“  
runtergelassen hat?**

Wenn Provider die Internet-Verbindung drosseln dürfen, bedeutet das für alle vernetzten Geräte im Haushalt wie Alarmanlagen, smarte Lautsprecher, Lichtsteuerung, und alles, was eine Internet-Verbindung benötigt, dass diese nicht mehr funktionieren werden, wenn Provider die Erlaubnis haben, die Internet-Verbindung zu drosseln. Laut den neuen Regeln der FCC sollen Provider in den USA das nämlich ohne Angabe von Gründen dürfen.



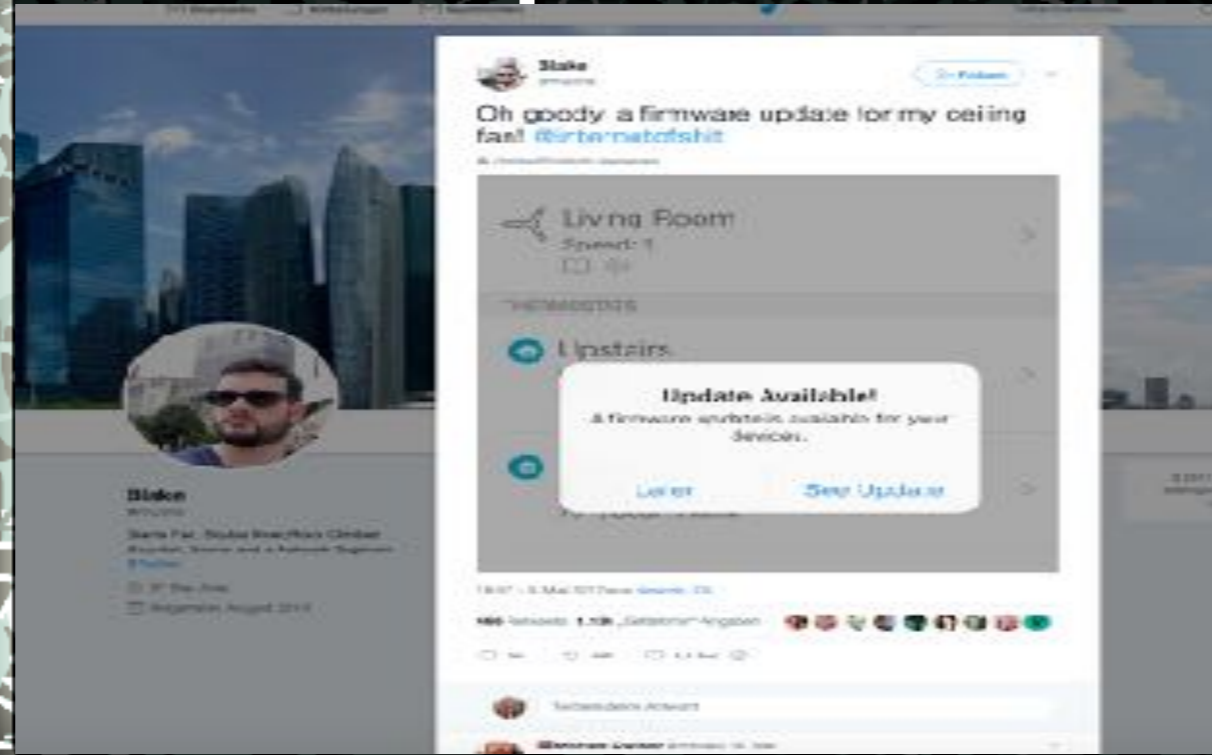
## **Weitere Probleme**

**Updates von IoT-Geräten  
im laufenden Betrieb**

# Updates



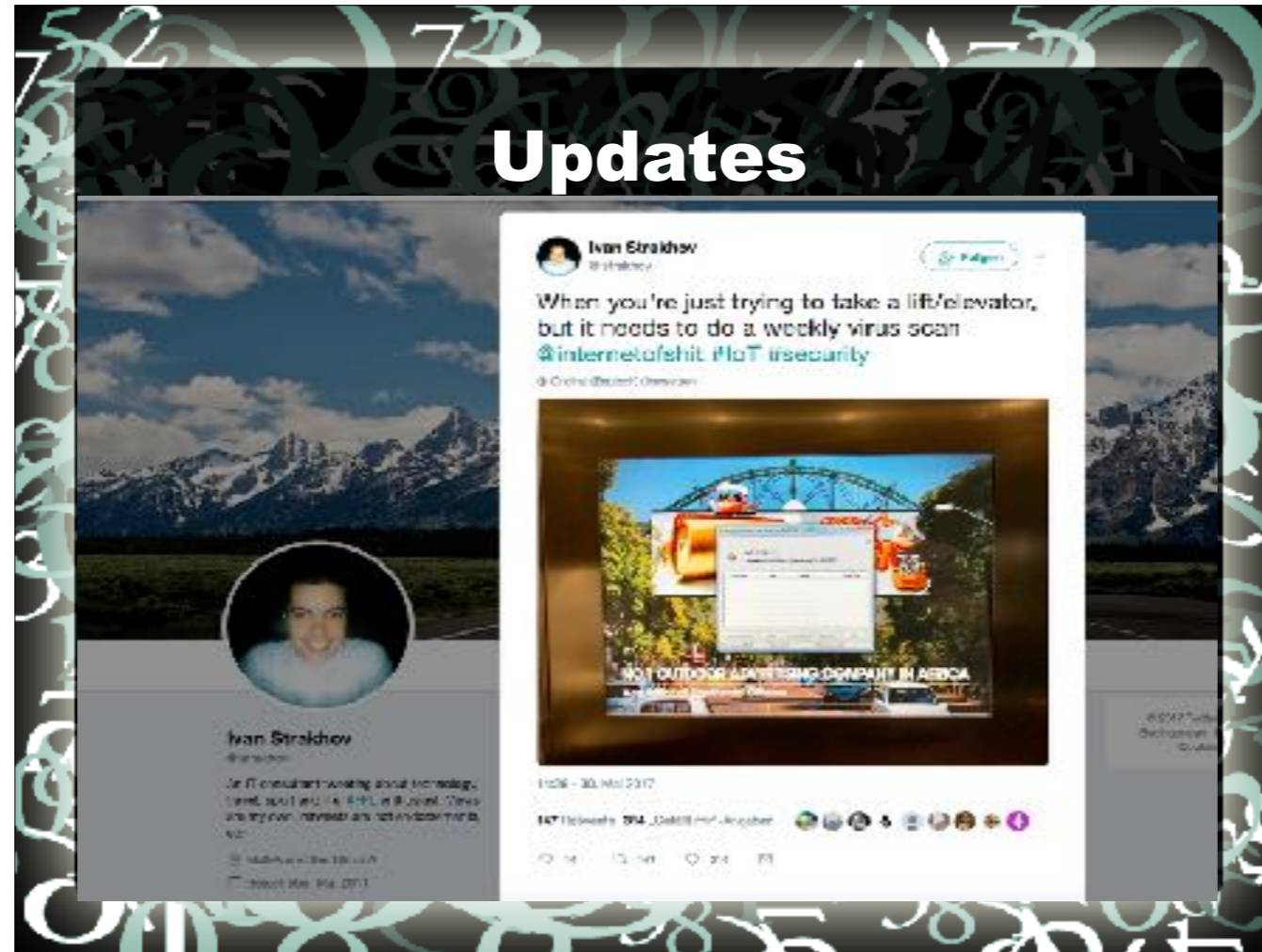
# Updates



# Updates



# Updates



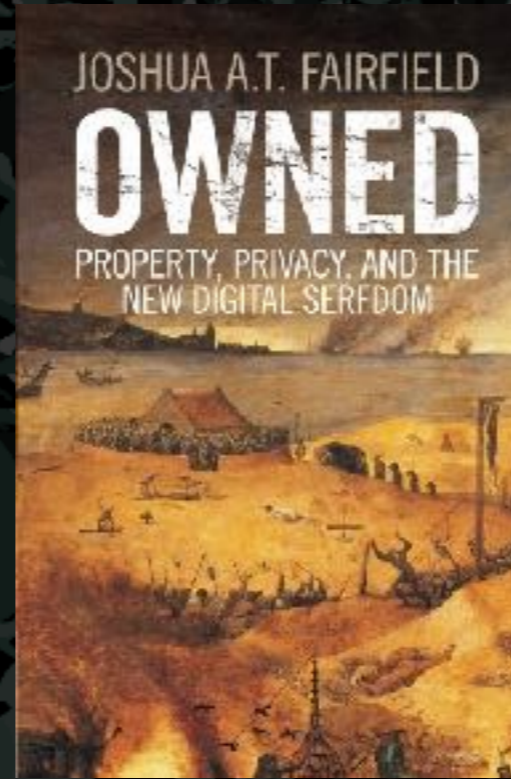
Auf der einen Seite geht es schneller, wenn ein Lift ein Update bekommt, als wenn er mehrere Tage außer Betrieb ist, damit ein Service-Techniker ihn wartet. Aber gleichzeitig kann einem Rollstuhlfahrer oder einer Mutter mit Kinderwagen das in dem Moment egal sein, wenn sie in einer Station steht und 30 Minuten lang warten muss, bis der Lift wieder funktioniert.....

## **Problem: Besitz**

**„Wir kontrollieren unsere Geräte  
nicht mehr,  
weil die Unternehmen denken  
und so handeln,  
als würden sie ihnen  
noch gehören.  
Sogar, nachdem  
wir sie gekauft haben.“**

Dann möchte ich noch ein weiteres Problem aufzeigen, was mit vernetzten Produkten, die wir erwerben, zunimmt: Wir geben zunehmend unsere Kontrolle ab. Wenn wir ein IoT-Produkt kaufen, kann es sein, dass wir es gar nicht mehr richtig besitzen, weil die Hardware von der Software des Herstellers abhängig ist. Joshua Fairfield hat dazu ein Buch geschrieben namens „Owned“.

# Problem: Besitz



# Sonos Lautsprecher



Ein Beispiel: Bei den Sonos Lautsprechern ist folgendes passiert: Wer den neuen Datenschutzbestimmungen nicht zustimmt, kann Sonos-Produkte künftig möglicherweise nicht mehr nutzen. Ein Opt-Out würde dazu führen, dass die Produkte auf Dauer „nicht mehr funktionieren“ würden, wie der Hersteller angibt.



# **Sonos Lautsprecher**

**Sonos One -  
Daten auch an Amazon Alexa und  
Google Assistant (ab 2018).**

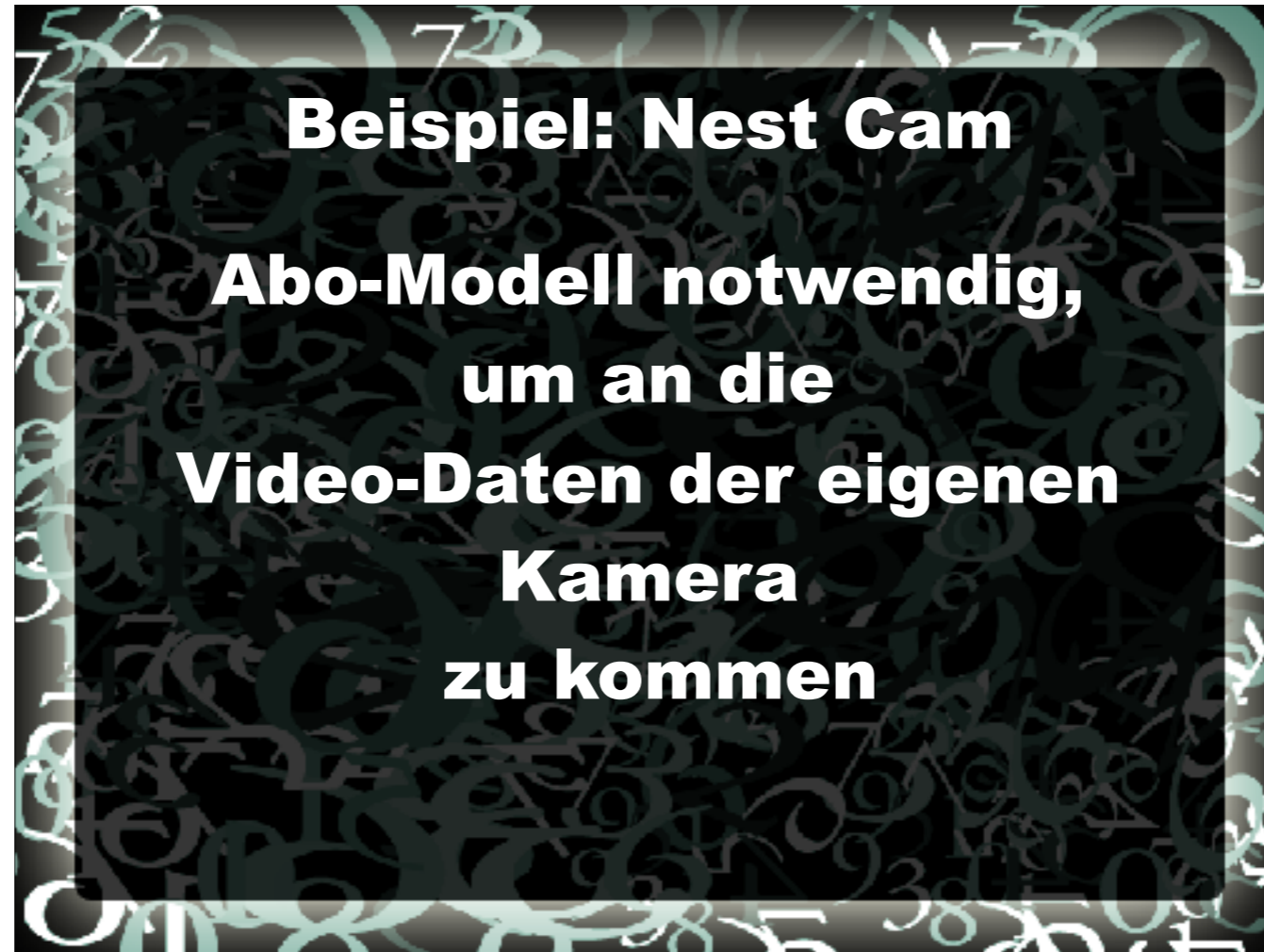
**Problem:  
Wer hat aller Zugriff welche Daten?  
Wer speichert diese wo?**

Dabei sendet Sonos One die Daten auch an Amazon Alexa und Google Assistant und man weiß als Nutzer nicht mehr, wer dann aller Zugriff auf welche Daten von einem hat und wo diese gespeichert werden.

## **Sonos Lautsprecher**

**„Das ist nicht fair, solange Unternehmen nicht damit beginnen, Nutzern eine echte Wahlmöglichkeit anzubieten.“**

**Lee Tien von der  
Bürgerrechtsorganisation EFF sieht in  
dem Vorgehen ein „wachsendes  
Problem“ im Bereich  
Konsumentenschutz.**



Nest Cam Indoor - Kaufpreis - 199 Euro - aber es gibt kein Video ohne Abo!

Abo - für den 10-Tages-Videoverlauf zehn Euro im Monat oder 100 Euro im Jahr für den 30-Tages-Videoverlauf 30 Euro im Monat bzw. 300 Euro im Jahr. Für jede Kamera weitere fünf Euro monatlich.

Problem 2: Funktioniert ohne Internet gar nicht



Als nächstes möchte ich zu einer anderen Unsicherheit kommen, nämlich der Unsicherheit, was mit den IoT-Daten eigentlich passiert. Hierzu möchte ich kurz über digitale Sprachassistenten wie Alexa oder Google Home sprechen.



Damit lässt sich viel mehr machen, als einfach nur Musik abspielen. Habe mit intensiven Nutzern gesprochen, was die alles damit machen. Es fängt in der früh an, sie lassen sich ansagen, wie der Tag wird: Von Wetter, über Termine bis hin zu Nachrichten und vorgelesen E-Mails

Am Weg zur Arbeit: Abrufen, ob irgendwelche Verkehrsbehinderungen vorhanden sind.



- \* Timersteuerung: Beim Grillen als Erinnerung zum Wenden.
- \* Einträge zur Einkaufsliste hinzufügen, entfernen geht leider derzeit aber nur über GoogleHome App.
- \* \* Telefonieren ist in den USA/GB schon ausgerollt, sollte bald auch hier kommen.
- \* \*Diktieren von e-Mails.

## **Sprachassistentin weiß...**

- \* Mit wem du sprichst/schreibst**
- \* Wann du außer Haus gehst/bist**
  - \* Was du einkaufst**
- \* Was für Musik du hörst/Serien du schaust**
- \* Wann du schlafen gehst/aufstehst**
- \* Über deine Hobbys Bescheid**

## **Was passiert mit den Daten?**

**Amazon, Google, Apple, Microsoft: Alle digitale Assistenten senden alle Sprachbefehle, die nach „Ok Google“ oder „Alexa“ oder „Hey Siri“ gesendet werden, zu den Firmen-Servern in den USA. Dort werden die Daten gespeichert.**



## **Gefahr für die Privatsphäre**

**„Für Nutzer ist nicht ausreichend nachvollziehbar, wie, in welchem Umfang und wo die erfassten Informationen verarbeitet werden. Auch ist nicht klar, für wie lange die Daten gespeichert werden.“**

**Deutsche Bundesbeauftragte für  
Datenschutz, Andrea Voßhoff.**

## The privacy risk of using a digital home assistant

By Sloan Schrage | Posted Jul 6th, 2017 @ 10:45pm

**\*“Die Daten, die über dich gesammelt werden, stellen einen unglaublich großen Wert für die Unternehmen, die diese Informationen sammeln, dar. Sie werden sie nutzen und auf verschiedene Art und Weise versuchen, diese Informationen zu monetarisieren.“**

**Quelle: [KSL.com](http://KSL.com)**

Viele denken sich jetzt vielleicht, dass es egal sein kann, wenn diese Daten auf US-Servern liegen oder was damit passiert. Aber für die Unternehmen ist das ein Wert und sie werden versuchen, es zu monetarisieren. Amazon probiert etwa bereits aus, wie man Audio-Werbung über Amazon Echo einsetzen kann und wie viel Unternehmen bereit sind zu zahlen, um an erster Stelle bei der Abfrage der Nutzer zu landen. Das wird früher oder später passieren.

A smart speaker, likely an Amazon Echo, is the central focus of the image. It is a dark, cylindrical device with a blue light ring at the top. The speaker is placed on a desk, with a white mug and some papers visible in the background. The entire image is framed by a decorative border featuring a pattern of numbers and symbols in a light green color. A white rectangular box with a thin black border is superimposed over the center of the image, containing the text.

**DO YOU TRUST YOUR DIGITAL  
ASSISTANT? LISTENING TECH  
JOINS THE PRIVACY DEBATE**

# **Gegenmaßnahmen**

**\* Sowohl Google Home als auch Amazon Echo verfügen über einen „Mute Button“ (Abschaltknopf)  
= man kann den Lauschvorgang bewusst unterbrechen**

**\* In den Einstellungen lassen sich die gesammelten Daten auch löschen und kontrollieren**

## **Gegenmaßnahmen**

- \*Verzicht auf Personalisierung: Dummy-Account zum Connecten des Geräts anstatt des täglichen Gmail-Accounts**
- \* Regelmäßige Firmware-Updates von digitalen Assistenten und dem WLAN-Netzwerk installieren**

## **Ja, aber...**

**\* Mitgelauscht wird offiziell nur nach dem Sprachbefehl „Hey Alexa“ oder „Ok Google“.**

**\* Datenschützerin warnt: „Risiko, dass die gespeicherten Daten nicht zu hundert Prozent sicher sind, bedenkt man die aktuellen Sicherheitslücken vieler Internetdienste“.**

# IT-Security

**Sowohl Amazon Echo als auch Google Home wurden bereits erfolgreich gehackt und der Mitlausch-Knopf ohne Zutun des Nutzers aktiviert.**

\*Dem Sicherheitsforscher Mark Barnes ist es gelungen, ein Amazon-Echo-Gerät mit dem Baujahr 2016 dazu zu bringen, permanent alles mitzuhören, was im Wohnzimmer gesprochen wird.

\*Datenschutzpanne mit Google Home Mini: Einschaltknopf wird deaktiviert -

Gerät lauschte bei Testgeräten mit, obwohl der Mute-Knopf aktiviert war. Der Fehler sollte mit einem Update bis zum Marktstart behoben werden.

# Überwachungskamera

**"Hola señorita!"**

Ich möchte noch weitere Beispiele aus dem Bereich der Überwachungskameras bringen, und damit zeigen, was fehlende IT-Security für Konsequenzen haben kann. Eine Niederländerin wollte mit ihrer IoT-Überwachungskamera ihr Haustier beobachten. Stattdessen wurde das Gerät gehackt und entwickelte ein scheinbares Eigenleben. Die Webcam dreht sich dabei und versucht offenbar, die Frau im Raum zu finden und sprach mit ihr auf Spanisch.





Weiteres Beispiel: Fabian Mittermaier von SEC Consult aus Wien knackte vor meinen Augen eine IP-basierte Überwachungskamera, die damit warb, „vandalismussicher“ zu sein. „Es ist, wie wir es aus dem Film kennen. Mit dieser Sicherheitslücke können Unbekannte völlig andere Bilder einspielen. Die Aufnahmen zeigen dann etwa, dass nichts passiert ist, während in Wahrheit gerade eine Bank ausgeraubt wird.“

Kamera als Sicherheitsobjekt = nutzlos



# Spionage im Kinderzimmer

VERBOTENE SENDEANLAGE

## Spionage im Kinderzimmer: Puppe Cayla wird verboten

von Barbara Wimmer 17.02.17, 11:14 [shroetbab](#) [Mail an Autor](#)



Die smarte Puppe Cayla wird in Deutschland verboten. Eltern sollen die Puppe zerstören, umsich nicht

### FEATURED



CHINA  
iPhone X Klon mit Android  
aufgetaucht

GADGET

## Stiftung Warentest sieht vernetztes Spielzeug "kritisch"

28.08.17, 12:24 [Mail an die Redaktion](#)

**Die Tester stuften drei von sieben  
geprüften Spielzeuge als sehr kritisch  
ein. Alle anderen als kritisch.**

**Darunter:  
Teddys, Roboterhunde, Puppen.**

## **Unsichere Funkverbindung**

**Drei der getesteten Spielzeuge benötigten für eine Bluetooth-Verbindung weder ein Passwort noch einen PIN-Code.**

**Folge: Jeder Smartphone-Besitzer könnte sich mit den Spielwaren verbinden, "um das Kind abzuhören, es auszufragen oder zu bedrohen", warnt die Stiftung Warentest.**

## **Unsichere Apps**

**Einige Apps, die zum Spielzeug gehören, erfassen die Geräte-ID des Smartphones, übertragen Nutzerdaten an Drittfirmen oder setzen Tracker, die auch das Surfverhalten der Eltern protokollieren können.**

## **Empfehlung**

**Ein nicht internetfähiger  
"dummer" Teddy  
ist in Zukunft  
die intelligentere Wahl  
als ein "smarter" Teddy.**



Sicherheitsforscher des britischen Unternehmens Pen Test Partners - Sicherheitslücke im Dildo - Diese ermöglicht es, vollständige Kontrolle über das Sex-Spielzeug zu erlangen und dem Benutzer auch bei der Verwendung zu beobachten



## **Smarter Dildo**

**Das Standard-Passwort: 88888888.**

**Wer vergessen hatte, dieses zu ändern, musste mit ein paar Zusehern mehr bei der Live-Übertragung rechnen.**



Lino  
@lino

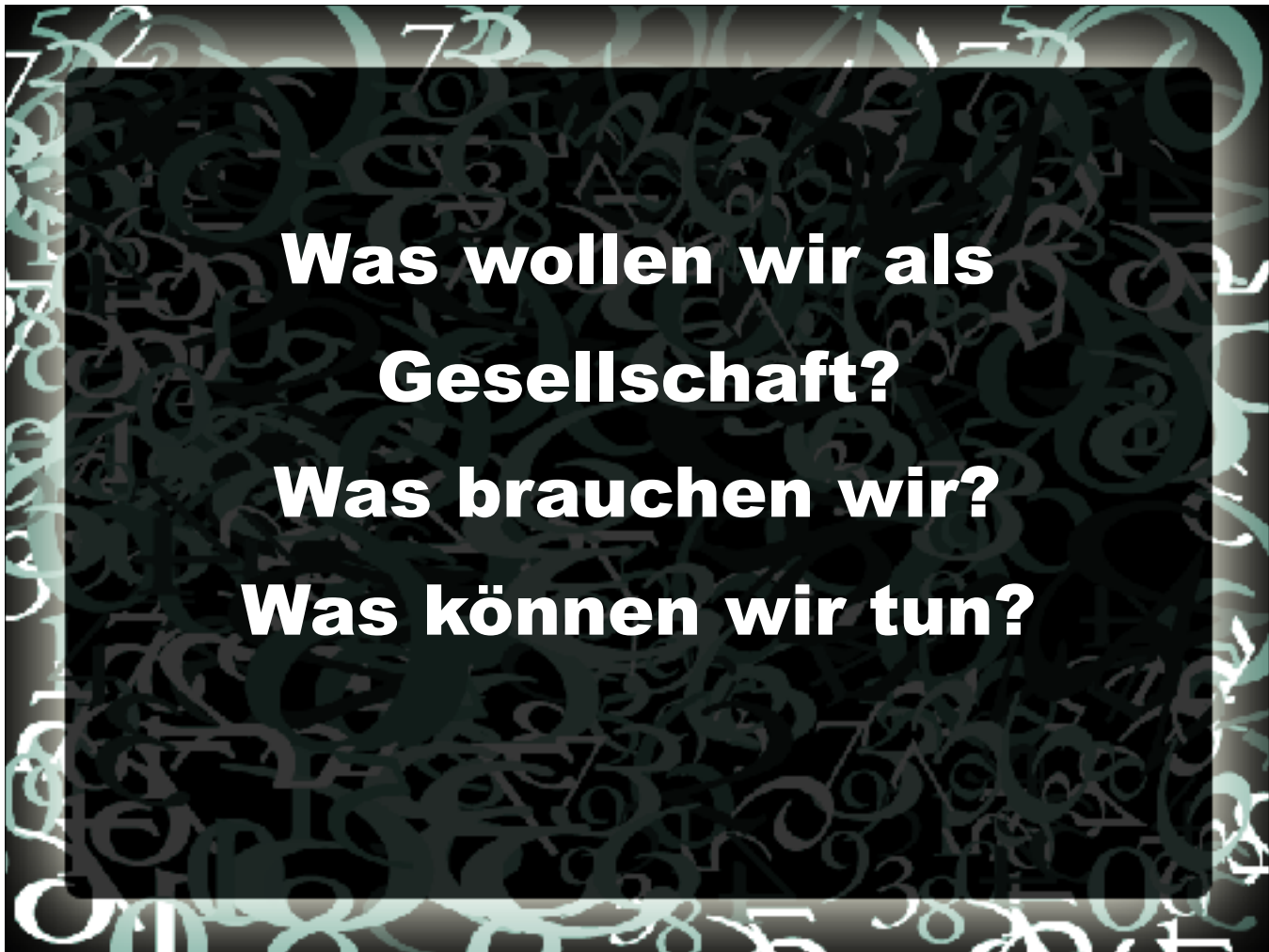
Folgen



<3 2017. Jemand hat einen Penetration Test bei einem Buttplug of Shit gemacht und das Ergebnis ist beschissen.

[pentestpartners.com/security-blog/ ...](https://pentestpartners.com/security-blog/)

18:47 · 19. Okt. 2017 aus Hamburg, Deutschland



**Was wollen wir als  
Gesellschaft?  
Was brauchen wir?  
Was können wir tun?**

## **Problem für Konsumenten**

**Im sogenannten „Smart Home“-Bereich, in dem Produkte auch für Endkonsumenten angeboten werden, gibt es für diese derzeit kaum eine Chance, festzustellen, ob sich ein Hersteller um Sicherheit bemüht hat oder nicht.**

## **Recht auf Offline!**

**Weil der Traktorhersteller John Deere  
Reparaturen nur gegen Bezahlung  
autorisiert, hacken immer mehr US-  
Landwirte ihr Fahrzeug mit ukrainischer  
Firmware.**

**Recht auf Reparatur**

**Analog dazu: Recht auf Offline**

## **Was wir brauchen**

**\*Nicht alles muss ans Netz!**

**Verpflichtender Offline-Modus  
für Haushaltsgeräte**

**wie Kühlschränke und Toaster**

**(aus: Jan Albrechts Empfehlungen der  
Grünen für mehr Sicherheit im Netz)**

## **Was wir brauchen**

- \* Digitale Produkt-Haftung:  
Kommerzielle Software-Hersteller  
haftbar machen, wenn sie bekannte  
Sicherheitslücken nicht schließen.**
- \* Software-Lizenzvereinbarungen, die  
eine Herstellerhaftung für  
Folgeschäden eines Hackerangriffs  
ausschließen, abschaffen.**

## **Was wir brauchen**

### **\* Online-Kaufrecht:**

**Softwarehersteller sollten Updates für Sicherheitslücken schnellstmöglich anbieten müssen und die Gewährleistung auf Nachbesserung und Umtausch um Mängel bei der IT-Sicherheit erweitern**



## **Was wir brauchen**

- \* Ein Rating-System für Security, ähnlich der Energieeffizienz-Labels bei Kühlschränken**

# **Gesetzliche Regulierung**

**Ab 25. Mai 2018**

**EU-Datenschutzverordnung**

**Mit**

**Privacy by Design**

**Privacy by Default**

## **Was jeder tun kann**

- \* Hinterfragen: Muss das wirklich ans Internet?**
- \* Falls nein: Nicht kaufen/dran hängen!**

## **Was jeder tun kann**

- \* Regelmäßige Updates: Alle Sicherheitspatches (sofern angeboten) einspielen**
- \* Getrenntes Heim-Netzwerk für IoT**
- \* Sichere Passwörter**

## **Was jeder tun kann**

- \* Open Software und Open Hardware unterstützen**
- \* Produkte, bei denen Daten lokal gespeichert werden bevorzugen**
- \* Eigene IoT-Tools basteln**

## **Was jeder tun kann**

- \* Clicktivism: Sich im Netz über den Hersteller beschweren hilft manchmal dabei, ihn von dummen Ideen wieder abzubringen.**

## **Was jeder tun kann**

- \* Sich für seine Rechte einsetzen und diese notfalls auch einklagen**
- \* Alternativen suchen und verwenden**

**Was jeder tun kann**

**Organisationen  
unterstützen, die sich für  
Privatsphäre und IT-  
Security einsetzen**



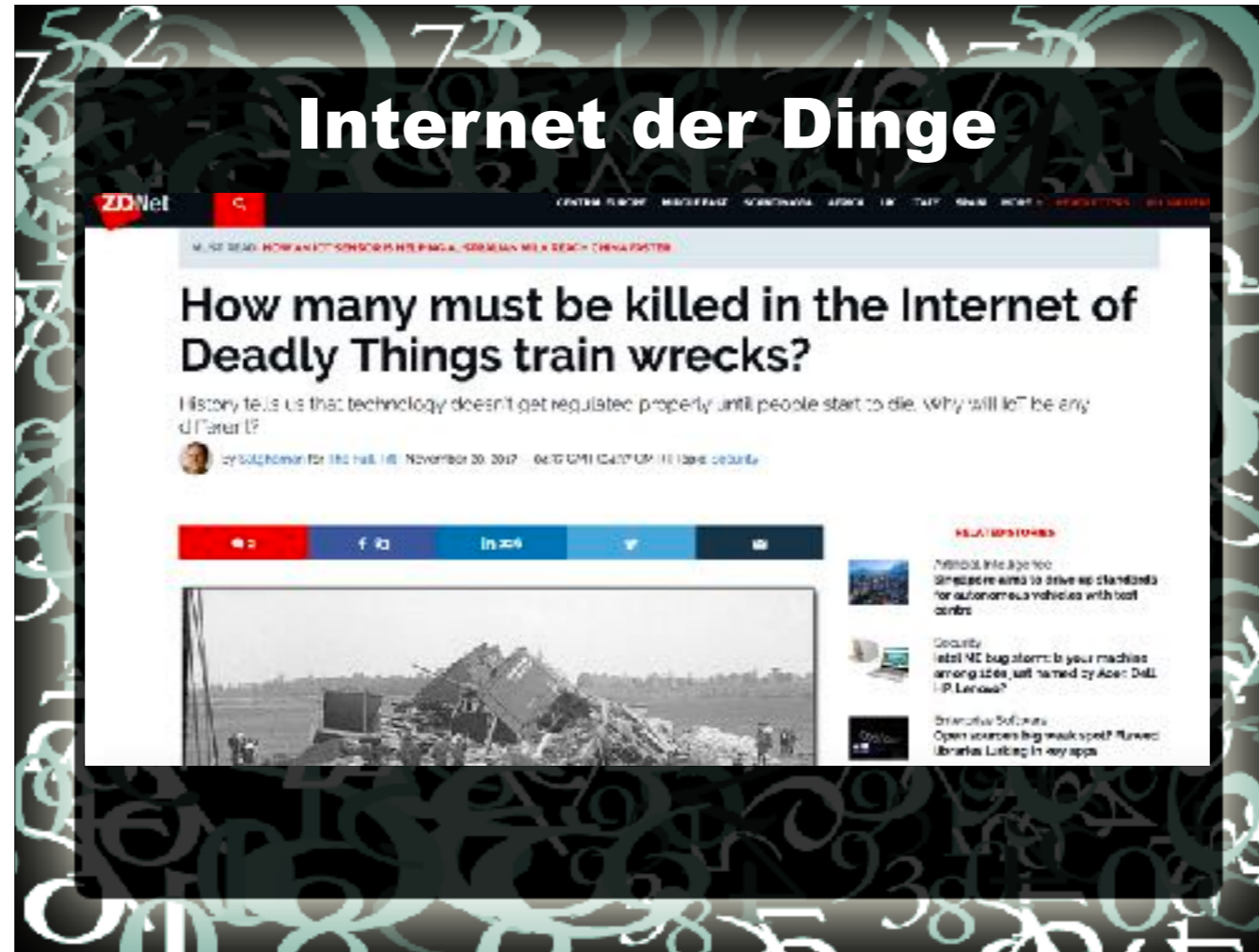
## **Was Entwickler tun können**

- \* **Privacy by Design fördern**
- \* **Security by Design fördern**
- \* **Von Anfang an bei der Produkt-Planung berücksichtigen**
- \* **Dinge anders machen, Verantwortung wahrnehmen**

## **Was IT-Security tun kann**

- \* Hersteller immer wieder auf die Probleme aufmerksam machen, damit IoT-Security ernst genommen wird**
- \* Sicherheitslücken melden**
- \* Forschung veröffentlichen (Open Science)**
- \* Bei der Entwicklung von IoT-Standards mitarbeiten**

# Internet der Dinge



Wir haben jetzt hauptsächlich der Konsumenten-Seite gesprochen. Aber durch fehlerhafte IoT-Security kann es auch zu Todesopfern kommen, wie etwa damals im Zeitalter der ersten Eisenbahnen, bevor es hilfreiche Signale und Bremsen gegeben hat. Phil Kernick stellt etwa die These auf, dass da zuerst etwas passieren muss, bevor ein Umdenken einsetzt. Ich hoffe es nicht, aber kann es definitiv nicht ausschließen.



**Dein Input?  
Deine Ideen?**

**Danke für eure Aufmerksamkeit!**

**Kontakt:**

**Twitter: @shroombab**  
**shroombab@gmail.com**