TeleTrusT
Pioneers in IT security.

TeleTrusT-interner Workshop

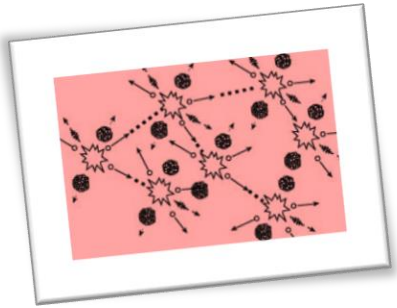
Essen, 29./30.06.2017

Sicherheit im Internet der Dinge

Mario Pietersz, PHYSEC GmbH

"Das Internet der Dinge ist kaputt" (Süddeutsche Zeitung)

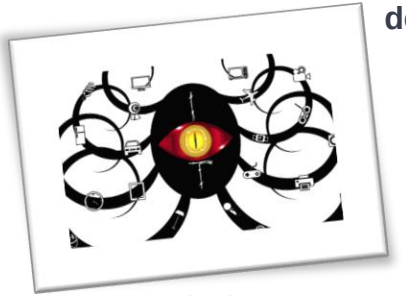
Ransomware



IoT goes nuclear

Hard-coded, factory default or easy-to-guess passwords

Hackers can take over medical equipment

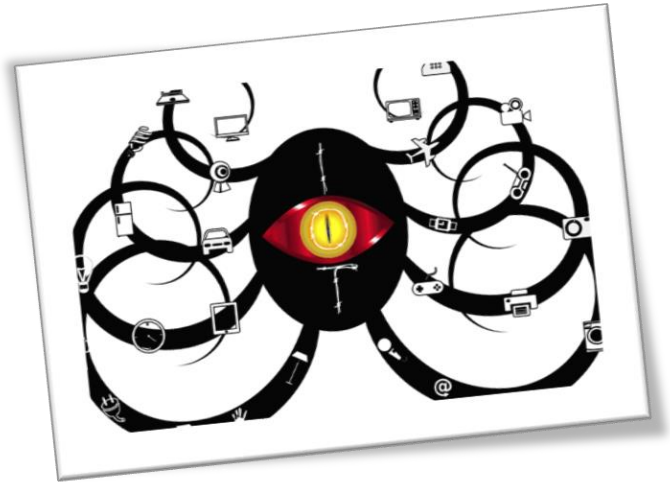


Mirai

http://codecurmudgeon.com/wp/iot-hall-shame/

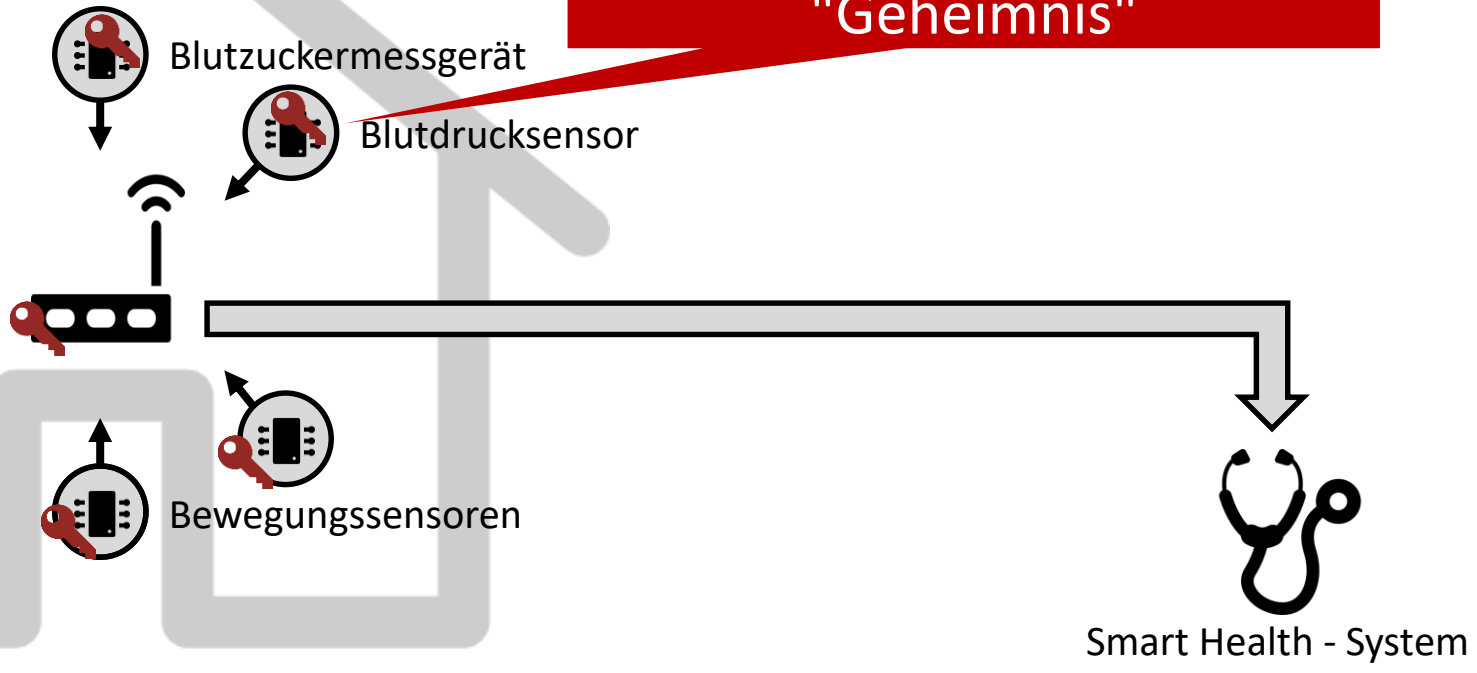
Mirai – Zukunft

- Was ist Mirai?
  - DDoS Botnetz
- Wie verbreitet es sich?
  - Ungesicherte Zugänge
- Wie wird es eingesetzt?
  - Websites/Router
- Ist die Gefahr gebannt?



1. Generation: Vorverteiltes Schlüsselmaterial

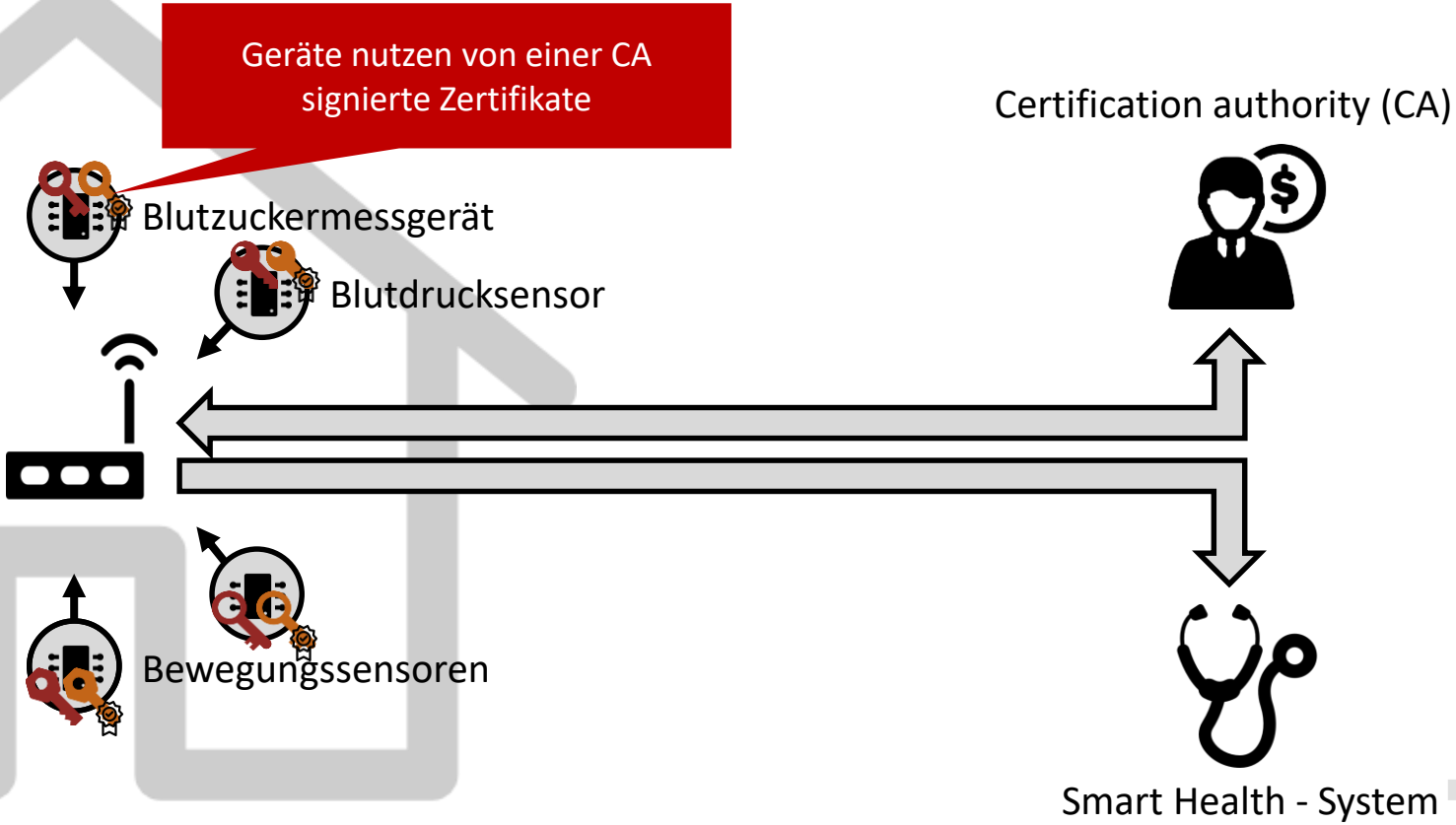
Alle Geräte nutzen das **gleiche** kryptografische "Geheimnis"



1. Generation: Vorverteiltes Schlüsselmaterial

	1. Generation: Vorverteiltes Schlüsselmaterial Einfach zu integrieren
Kosten	+ Geringe **Produktionskosten** + Günstige Hardware + Keine Administration
Security	– Leicht zu attackieren – Einzelner Angriff **skaliert** auf gesamte Produktreihe
Usability	– **Anwender** soll Schlüssel ändern

2. Generation: Public-Key-Infrastruktur

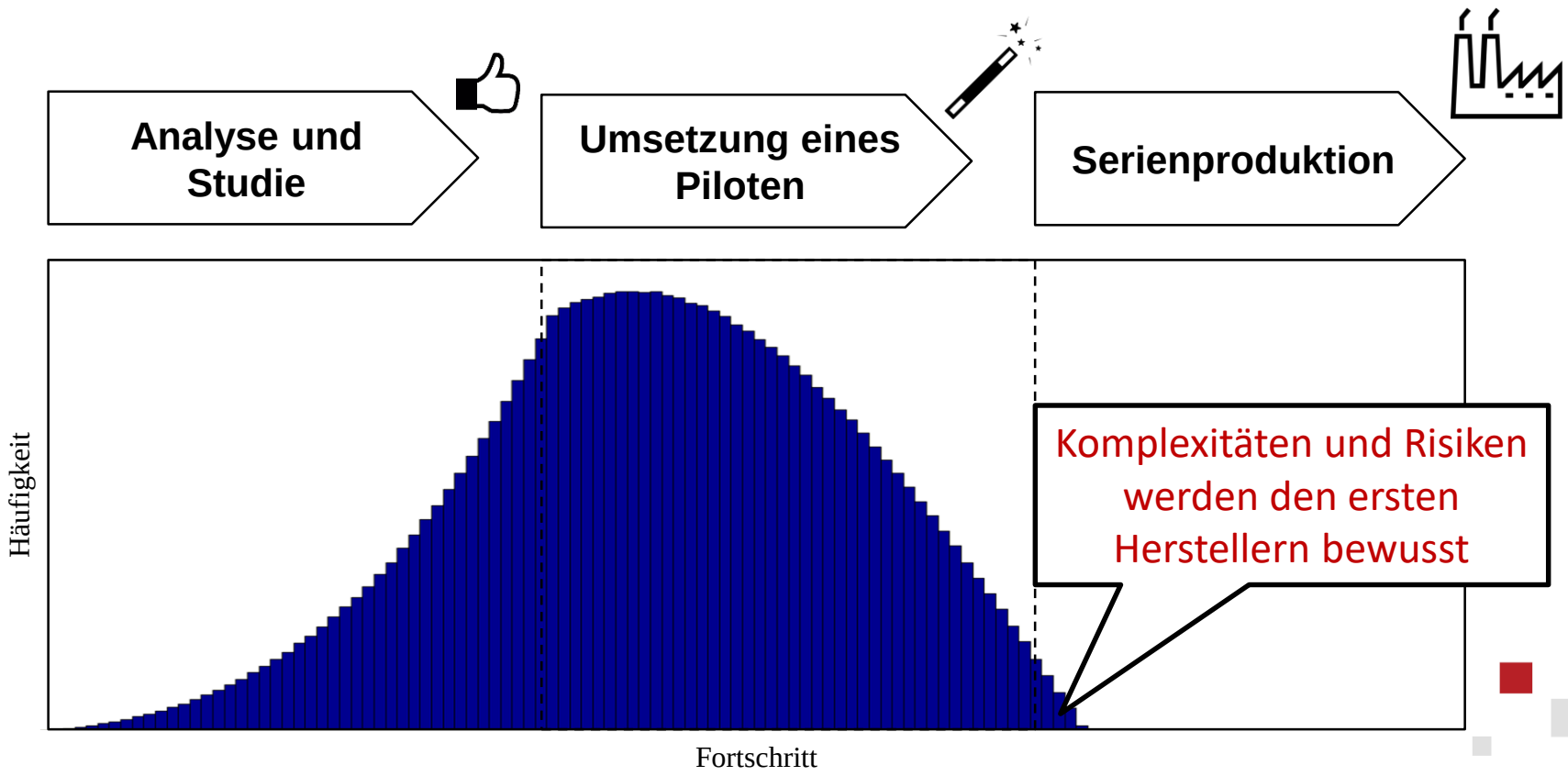


2. Generation: Public-Key-Infrastruktur

	1. Generation: **Vorverteiltes Schlüsselmaterial** Einfach zu integrieren	**2. Generation:** **Public-Key-Infrastruktur** Sichere Kommunikation
Kosten	+ Geringe **Produktionskosten** + Günstige Hardware + Keine Administration	– Supply-Chain **Komplexität** – Endgeräte Hardware – Infrastrukturkosten
Security	– Leicht zu attackieren – Einzelner Angriff **skaliert** auf gesamte Produktreihe	+ **Individuelle** Schlüssel – Zentrale Architektur
Usability	– Anwender soll Schlüssel ändern	+ **Plug & Secure**

Neue Kosten & Risiken

Phasen der Digitalisierung



Abwägung zwischen Sicherheit und Kosten

1. Generation: **Vorverteiltes Schlüsselmaterial** Einfach zu integrieren	2. Generation: **Public-Key-Infrastruktur** Sichere Kommunikation
+ Geringe **Produktionskosten** + Günstige Hardware + Keine Administration	– Supply-Chain **Komplexität** – Endgeräte Hardware – Infrastrukturkosten
– Leicht zu attackieren – Einzelner Angriff **skaliert** auf gesamte Produktreihe	+ **Individuelle** Schlüssel – Zentrale Architektur
– Anwender soll Schlüssel ändern	+ **Plug & Secure**

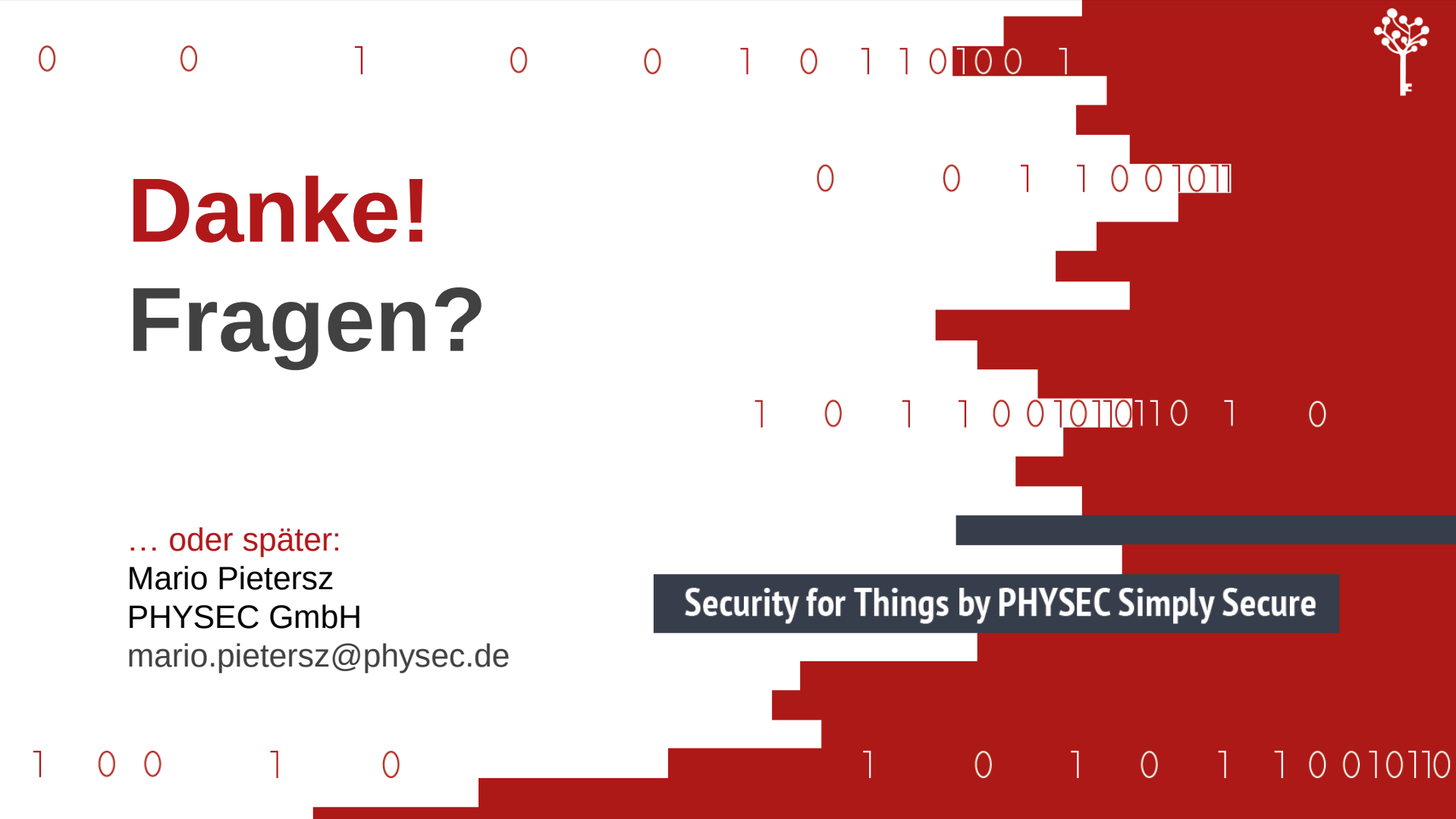
Neue Kosten & Risiken

Usability

Probleme und Herausforderungen

- Probleme
  - IoT-Sicherheit funktioniert nur mit ordentlichem **Schlüsselmanagement**
  - **Komplexitäten** und verbundene Risiken werden aktuell noch oft **unterschätzt**

- Herausforderungen
  - Market-Education
  - Mindestanforderungen, Whitepaper



Danke!
Fragen?

… oder später:

Mario Pietersz
PHYSEC GmbH
mario.pietersz@physec.de

Security for Things by PHYSEC Simply Secure