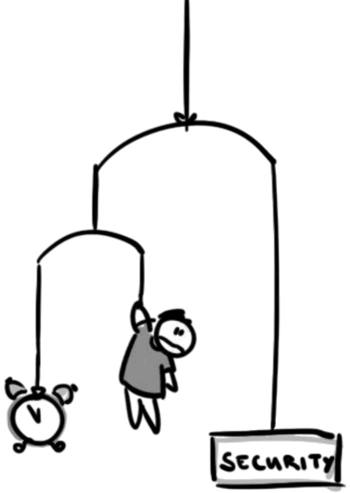
**CONSTANZE DIETRICH**
Beuth Hochschule für Technik &
Technische Universität Berlin
[@WeddingTrash // constanze.die@gmail.com]



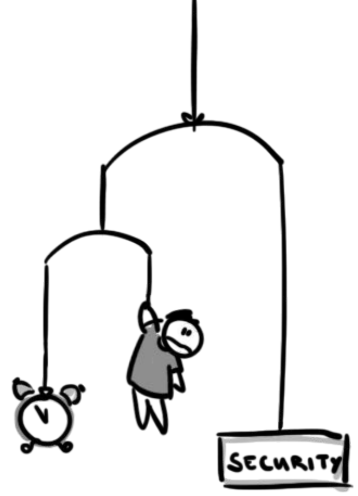
RIPE IoT Roundtable Meeting, 21 September 2017

# What’s now, what’s next?

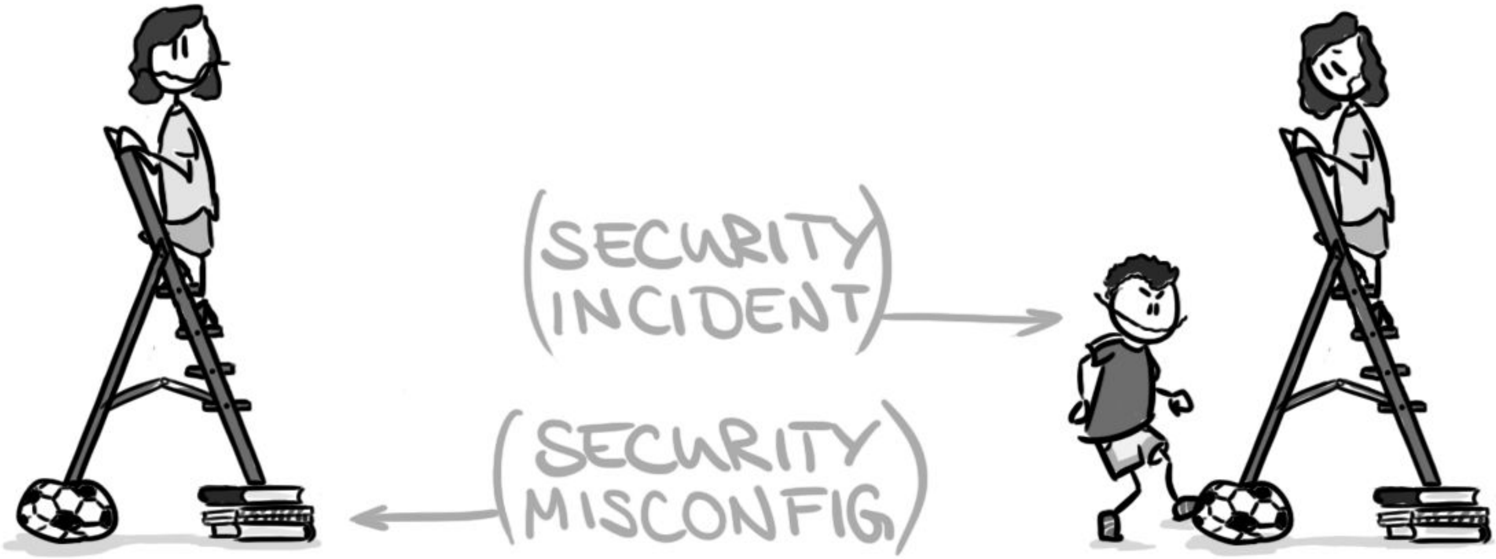
## Lessons Learned by Exploring Security Misconfigurations among Operators

# Outline

1. Why we’re here: The Issue
2. How we got here: The Empirical Approach
3. Who got us here: The Respondents
4. What’s now? Preliminary Findings  
   Threats for the IoT
5. What’s next? A few Ideas



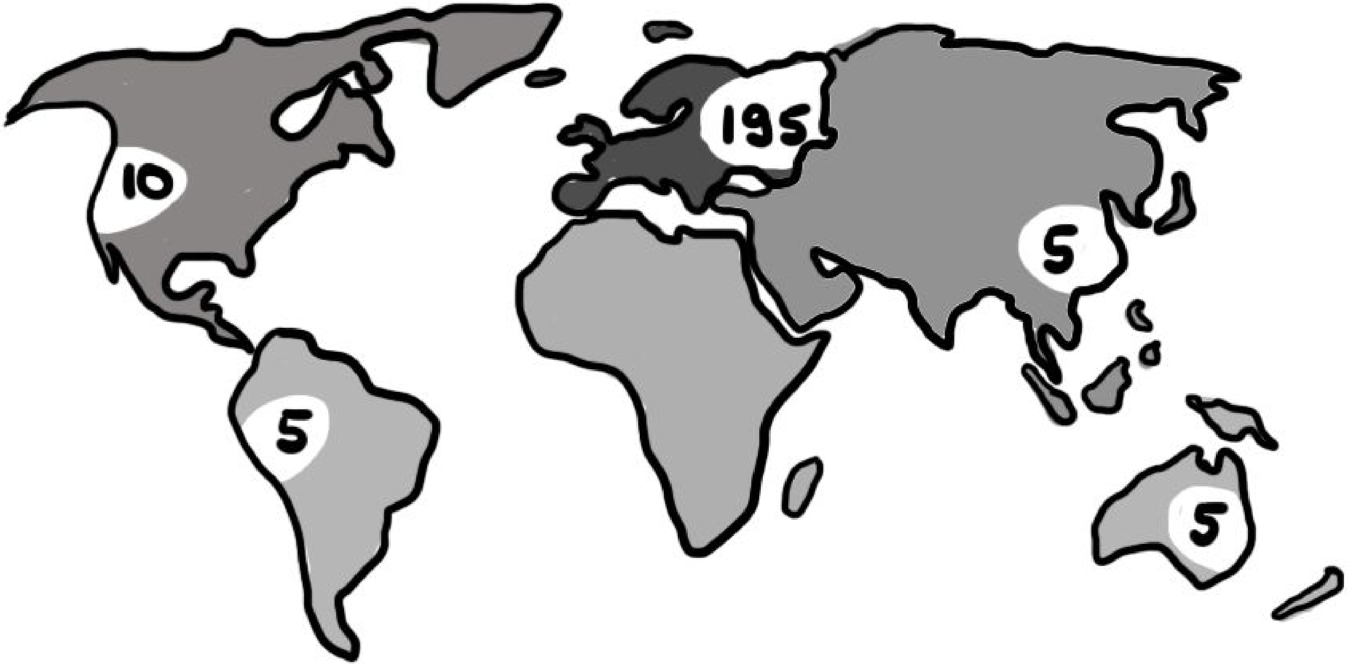
# The Issue

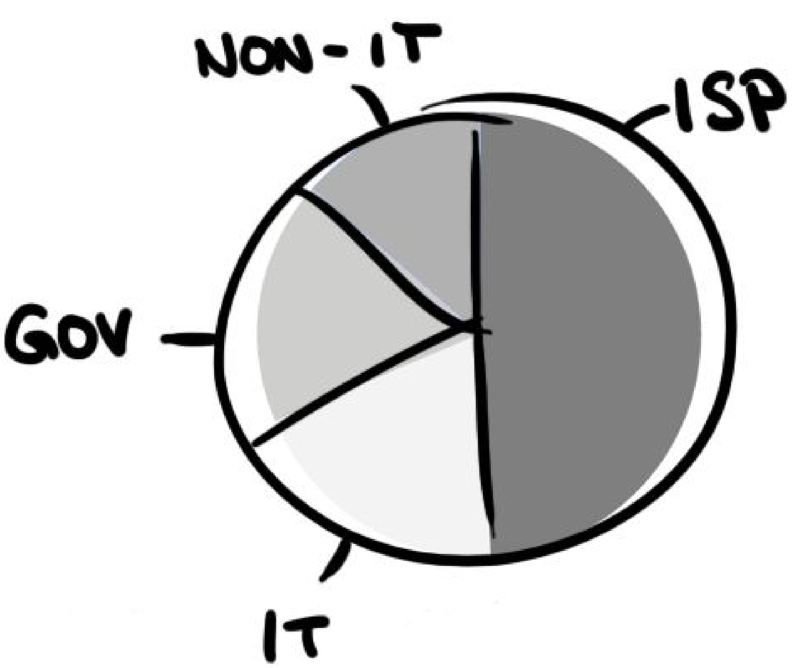


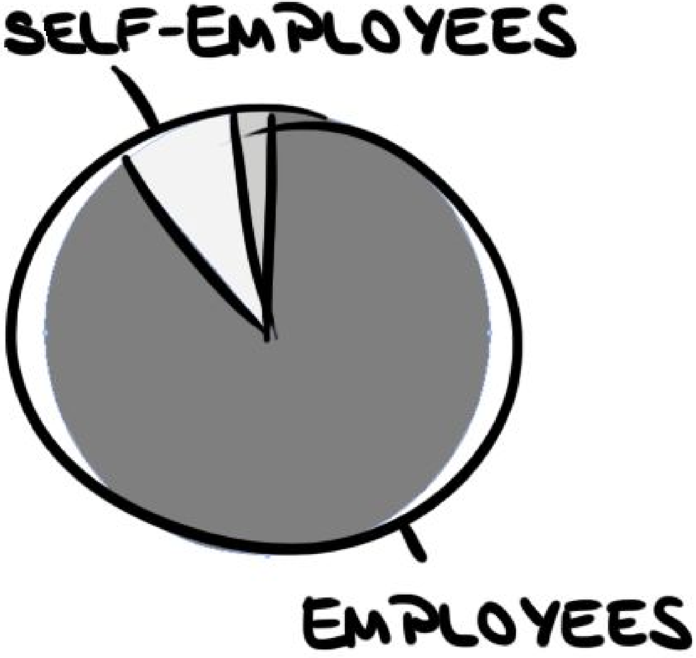
# The Empirical Approach

1. Interviews and focus group
2. Presentation of the findings at RIPE 74
3. More interviews!
4. Anonymous online survey

# The Respondents




NON-IT
ISP
GOV
IT


SELF-EMPLOYEES
EMPLOYEES

# Findings

- 220 operators have encountered security misconfigrations:
  1. Bad or publicly known passwords 86%
  2. Missing or delayed updates 83%
  3. Faulty assignment of permissions 82%

# Findings

- 196 operators made security misconfigurations:
  1. Missing or delayed updates 63%
  2. Faulty scripting 58%
  3. Faulty firewall configuration 57%

# Findings

- Personal reasons:
  1. Lack of Knowledge 79%
  2. Lack of Experience 76%
  3. Having other priorities 67%

# Findings

- Environmental reasons:
  1. Sole responsibility 77%
  2. Insufficient quality assurance 73%
  3. Time pressure 69%

# Findings

- System-related reasons:
  1. Usage of defaults 60%
  2. Complexity of a system 54%
  3. Legacy support 47%

# Threats for the IoT

> "Availability was the biggest issue
> and it is the lowest of concerns regarding security."
>
> – respondent #191

# Threats for the IoT

“This is fine.”

# Threats for the IoT

“What shall we do with the ops-less network?”

− my supervisor (singing)

# What’s next?

- Security incident “fire drills” for management?

“One incident gets your boss to improve security.
Two incidents gets their boss to improve security.
Three.... You get it, don't you?”

− respondent #120

# What’s next?

- Troubleshooting courses for evolving operators?

“[In school] They only focus on installing and putting things together. Unless you learn to become a car mechanic or so. Where broken is the state you start with.”

− interviewee #11

# What’s next?

- Postmortems. Blameless!

“Usually its a question whether the risk assessment was correct or needs adjustment and following that sometimes security measures are enhanced.”

− respondent #52

# Conclusion

What’s now?

Confidentiality Integrity Availability
Expiry Dates
DevOps und Userators

Further Evaluation

What’s next?

Education
Preparation
Post-processing