itdesign

Public Cloud Security

"Baking Cloud Architects - many tools, no fools"

Dr. Tobias Hüttner

Who am I ?

Dr. Tobias Hüttner
CIO
tobias.huettner@itdesign.de

- computer science "Diplom" at Tübingen university
- PhD in computer science
- Various management positions in IT operations, IT service management since then
- Now: engaged in public clouds and SaaS provisioning

Some words about itdesign ...

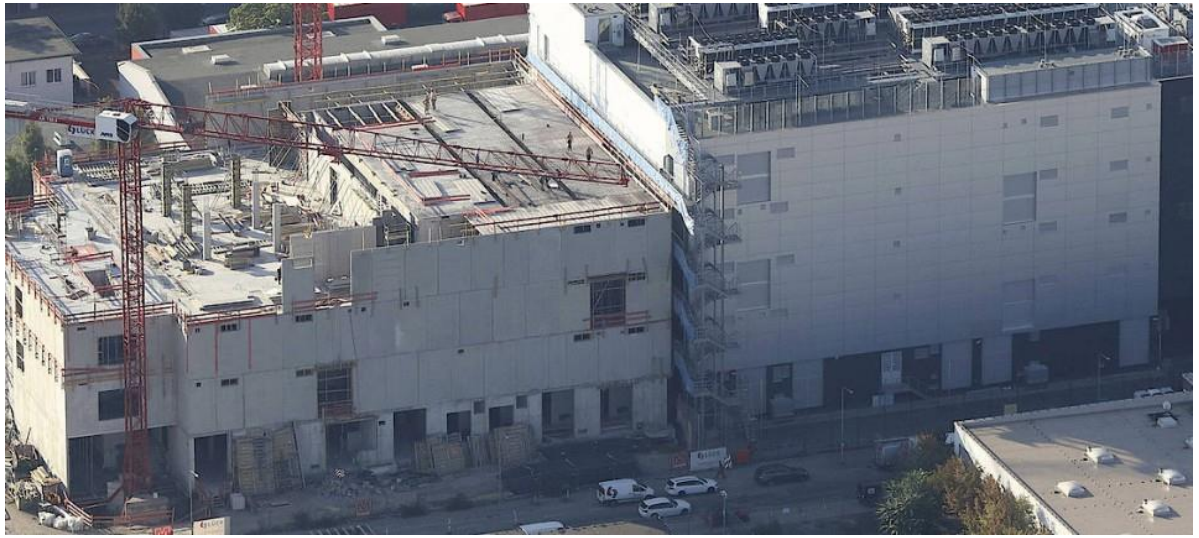
itdesign

Topics

The ingredients:

- **Knowledge - "People without experience are fools"**
- **Patterns - "same solution for similar problems"**
- **Automation - "people make mistakes"**
- **Cloud Programming - "functions are the new servers"**
- **Use instead of build - "many tools – no fools"**

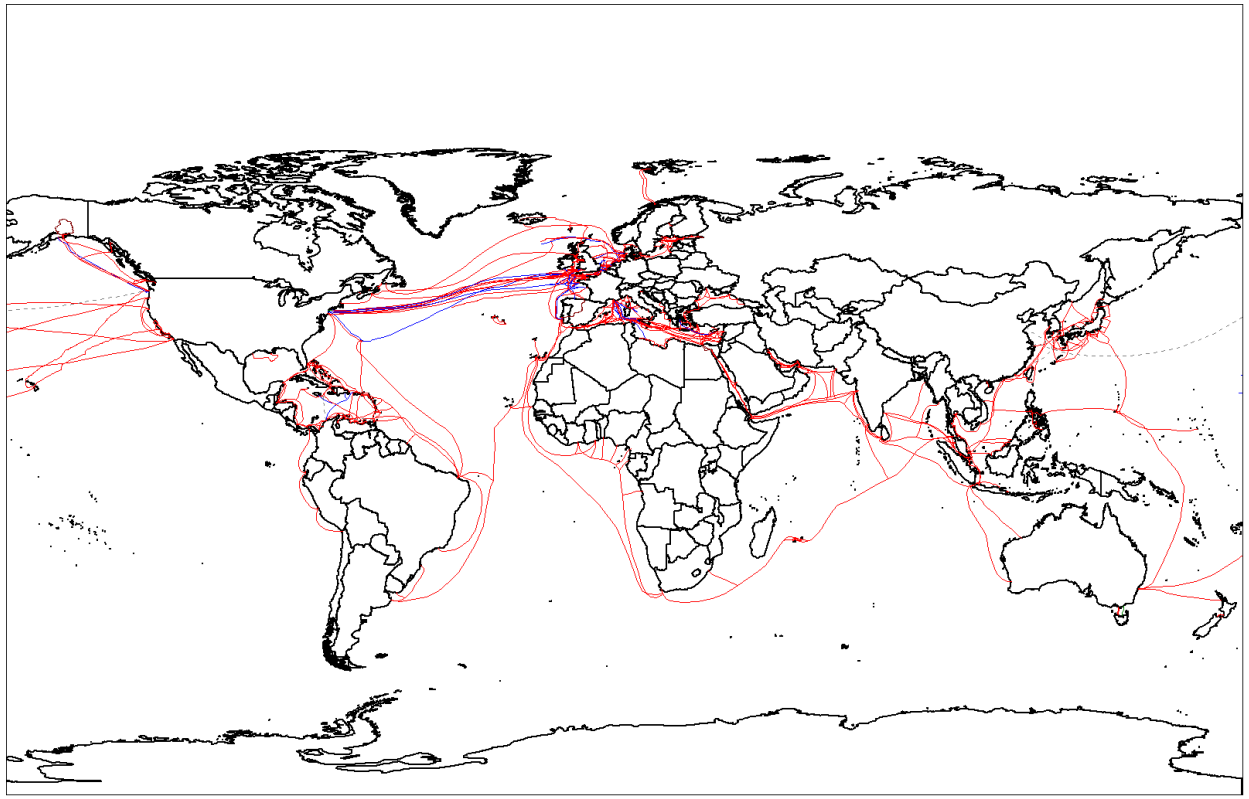
Motivation: those are our data centers …

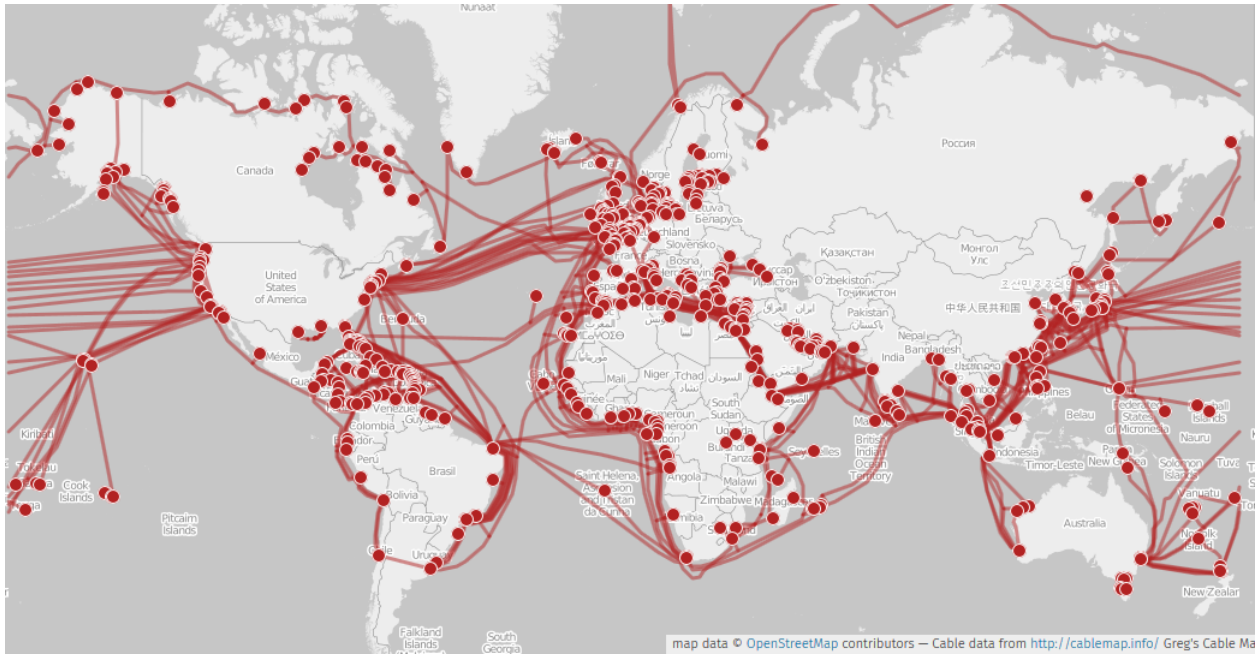


PUE = Total Facility Power / IT Equipment Power

itdesign

.. and this is our network ...





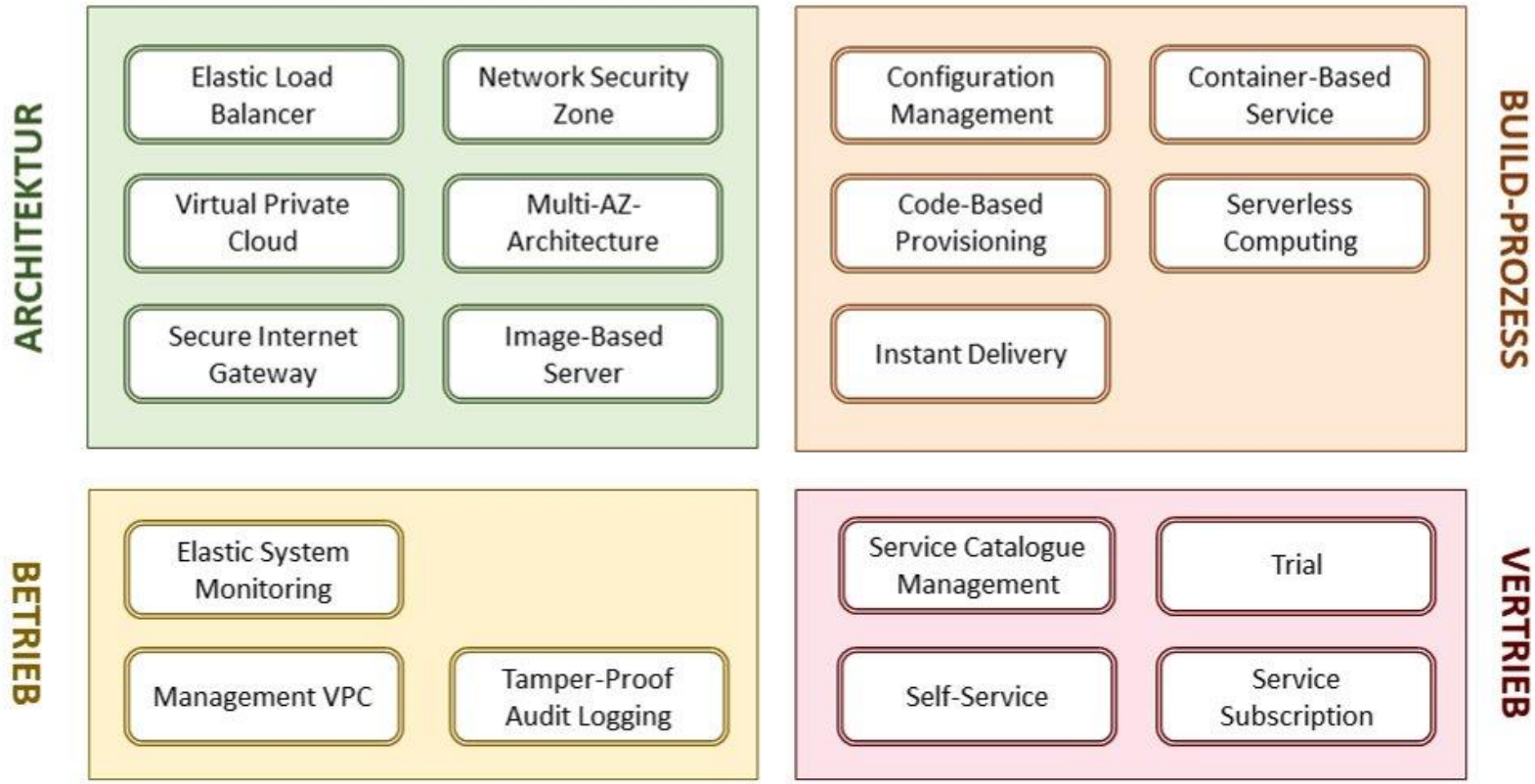
itdesign

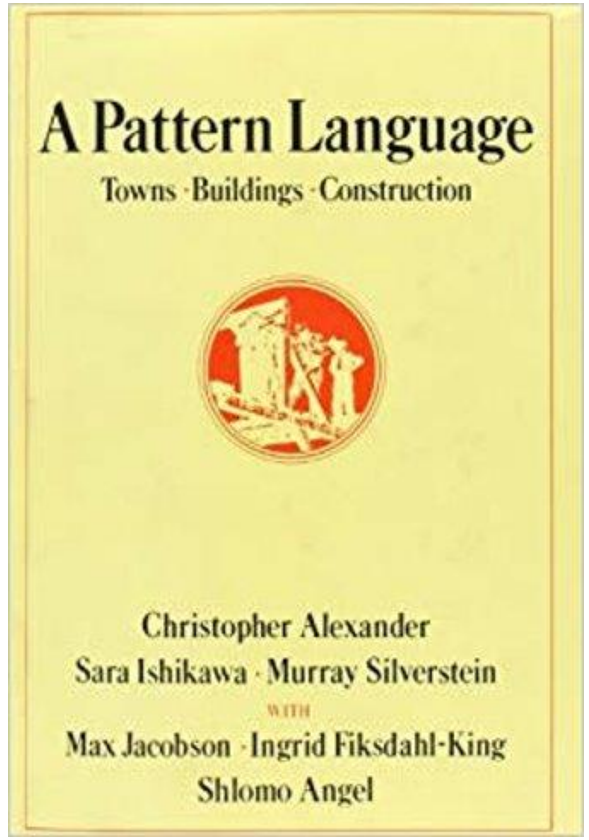
Knowledge

- Public Clouds are not just another data center – they arec eo systems on their own that need to be mastered
- We therefore organized a lecture "Public Cloud Computing" over one semester 2019/2020
- We educated not on Powerpoint – alle participants solved practical exercises of creating and operating workload
- We were very satisfied with the results – we had solutions for the major public clouds AWS, Azure and GCP – and one team also tried the university driven "BW Cloud"
- Education and Knowledge is one corner stone for inherent IT security !

Patterns

- **"same solution for similar problems"**





itdesign

Automation

- Classic way: scripting – imperativ way of telling step by step what to do
- In public clouds: **infrastructure as code**
  - Declaration what shall be deployed
  - The cloud takes care about the details of the deployment e.g. IP addresses, network settings, etc.
  - Scaling means changing the infrastructure declaration : "give me 5 more of those"
- Patterns and Automation generate IT security
  - Proven patterns can be repeated without manual interaction that always has an error probability
  - Especially when it comes to big numbers, people make mistakes or don't have overview any more ...

Cloud Programmming

- **"functions are the new servers"**
- **You don't need a virtual machine / a server for executing code any more – you can AWS Lamda, Azure Functions or Google Functions instead**
- **Even complicated environments like databases or Kubernetes clusters are available as managed services that you don't need to operate on your own**
- **On the other hand, the major public cloud providers are thouroughly certified and provide IT security (e.g. ISO 27001 certificates) for these building blocks**
- **Using such parts as patterns in your architecture increases IT security tremendously – the amount of IT security incidents is nowadays lower in public clouds than on premise (*bitkom* cloud monitor)**

Use instead of build

- IT security relevant functionality is available in public clouds as managed services
- Example AWS
  - Base Layer: VPC – virtual private cloud – network separation patterns
  - Next Layer: ELB – Elastic Load Balancing – connection to the world
  - Next Layer: WAF – Web Application Firewall – next generation firewall, enhancable with AWS marketplace rulesets (e.g. from F5)
  - Next Layer: Guard Duty – SIEM system
  - Next Layer: Detective – KI based anomaly detection of your complete environment
  - AND: **we talk in terms of implementation times of hours – and no longer man years !**

Thank you !

… and if there are questions: just ask now …

Or: tobias.huettner@itdesign.de