FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Cyberangriff? Notaus!

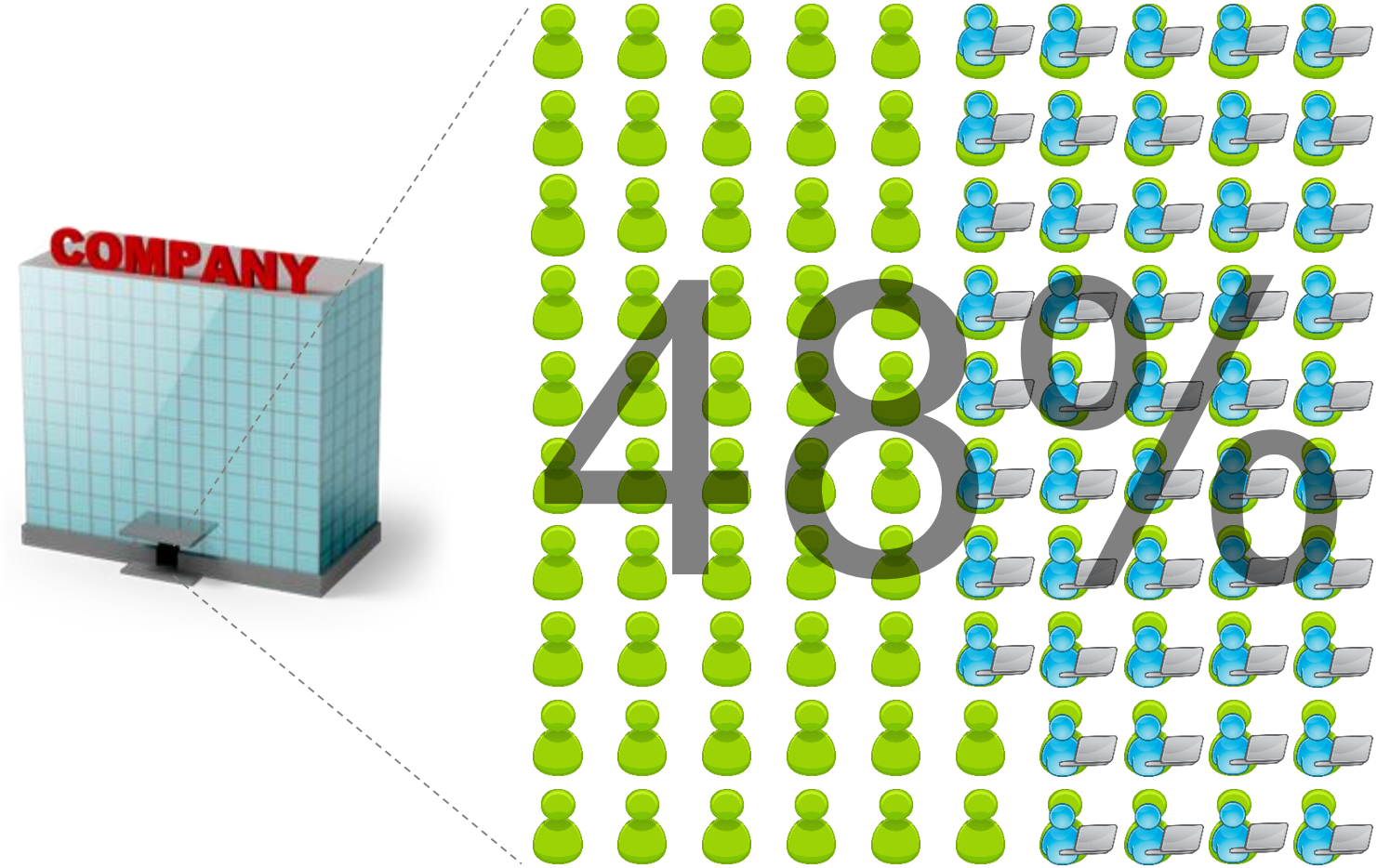
Rene Wölker
ISB / Security Consultant
International School of IT Security / RUB

IT Forensik
FH Aachen

Agenda

- Einleitung
- Idee
- Konzept
- MVP

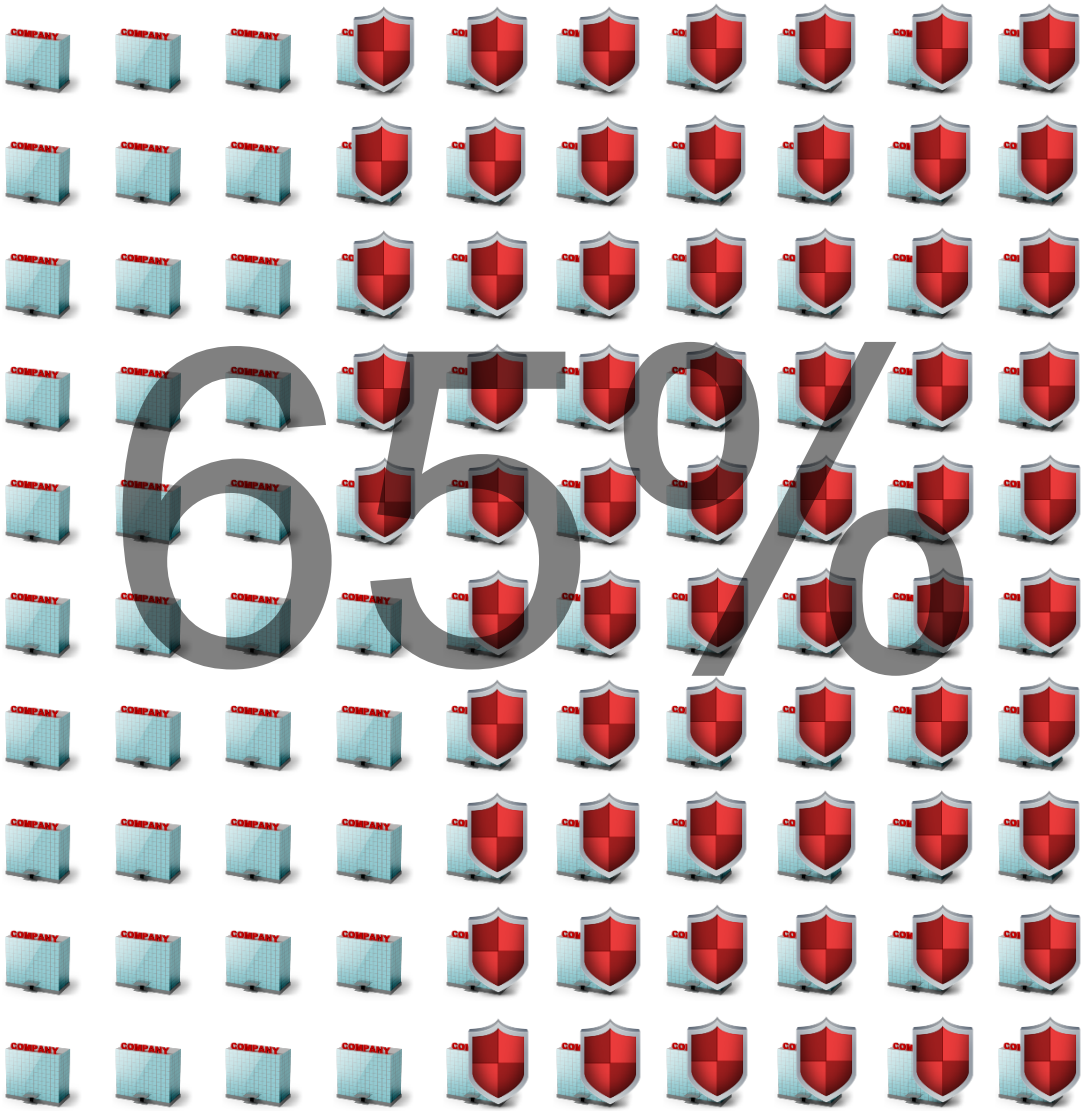
Einleitung – Ausgangsituation



48% arbeiten am Computer

vgl.: Bitkom Digital Office Index 2018

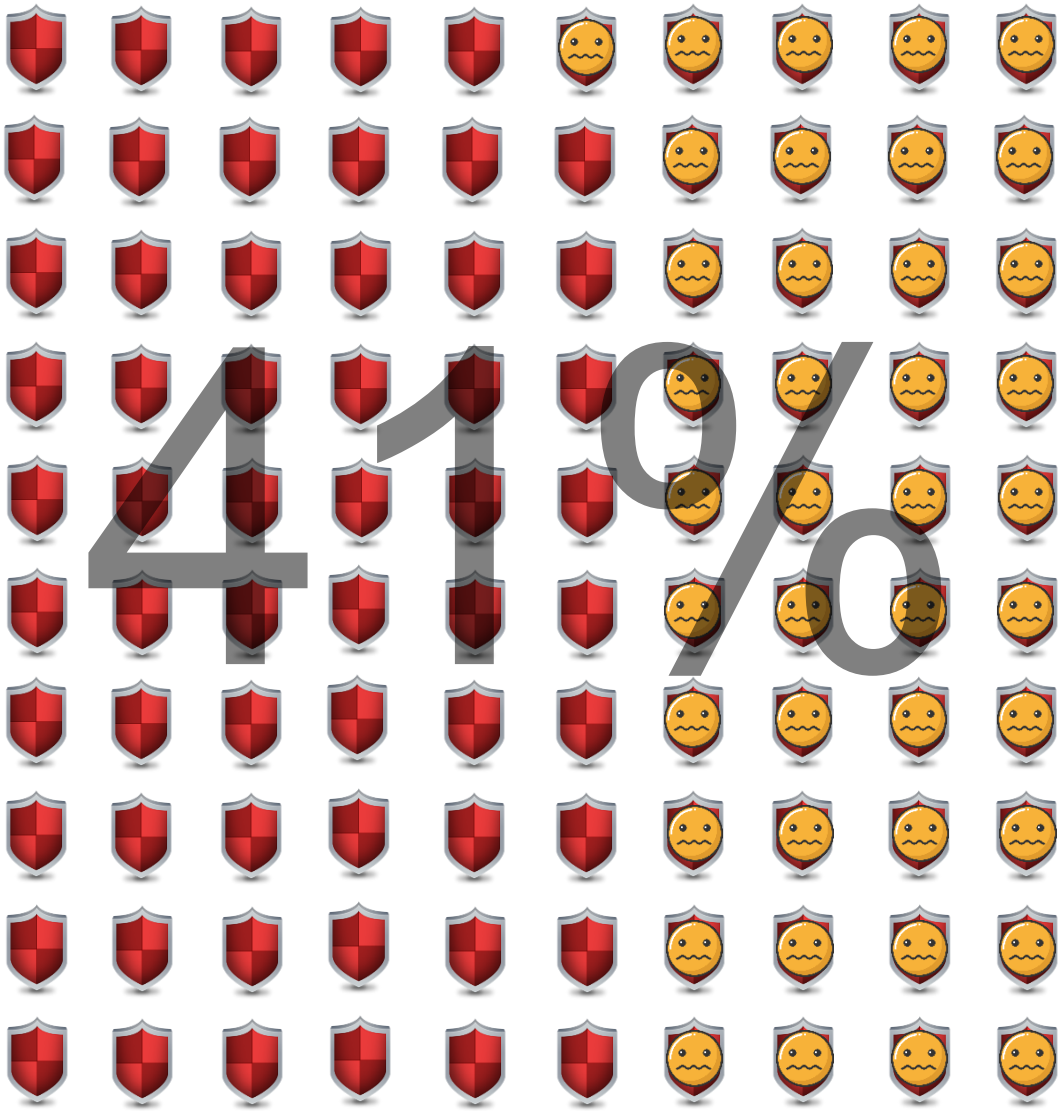
Einleitung – Ausgangsituation



65% der Unternehmen hatten 2017 Incidents

Vgl.: 2017 IT Risks Report, netwrix

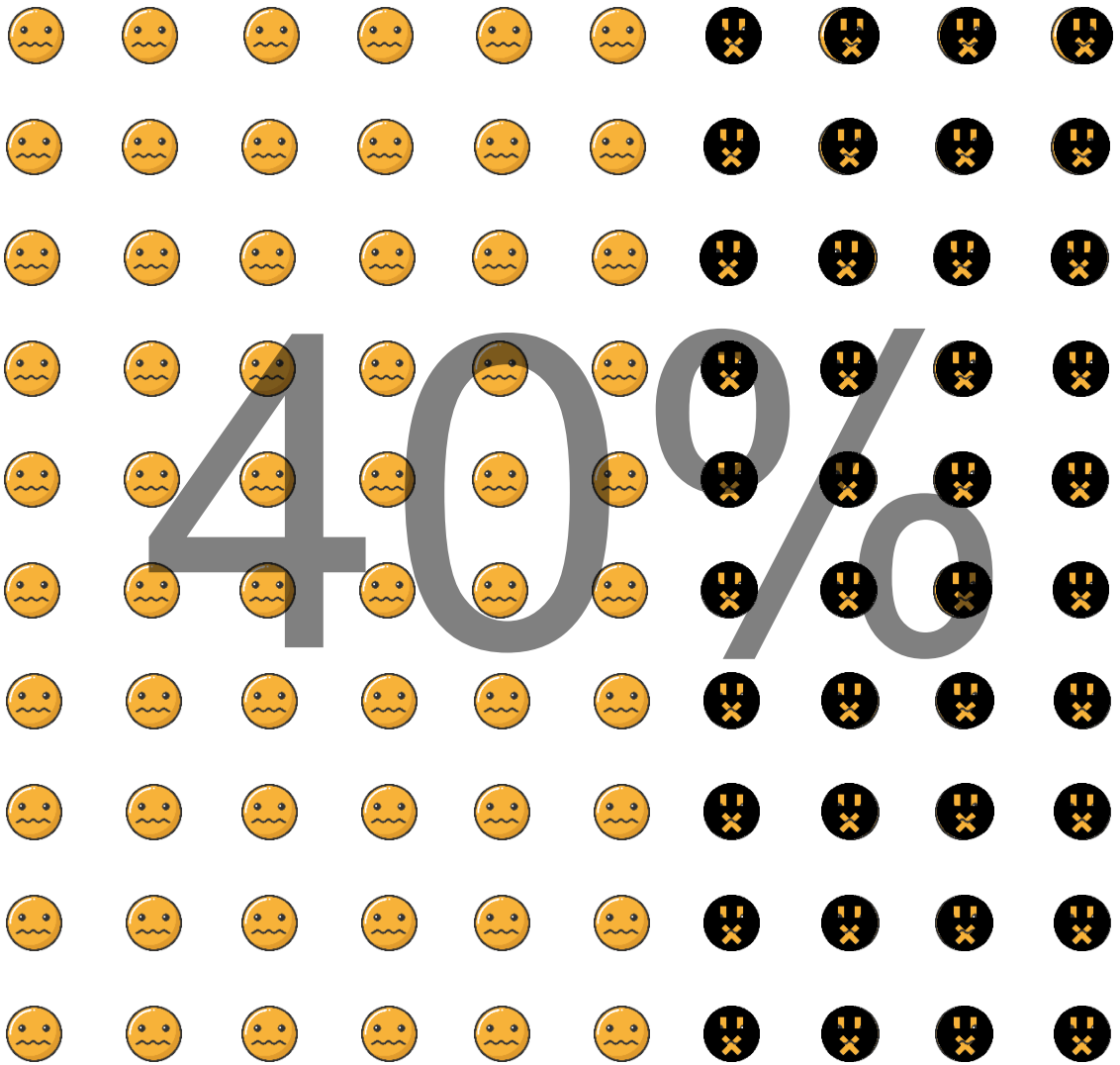
Einleitung – Ausgangsituation



41% der Incidents durch menschliche Fehler

Vgl.: 2017 IT Risks Report, netwrix

Einleitung – Ausgangsituation



40% der Mitarbeiter würden nicht melden

Vgl.: 2017 IT Risks Report, netwrix

Faktor Mensch

- EIFOK
  - error in front of keyboard
- ERROR-40
  - Fehler befindet sich 40 cm vor dem Monitor
- Error in Layer 8
  - Erweitertes OSI Model
- PEBKAC
  - problem exists between keyboard and chair

- Anwender nicht das Problem, sondern ein Teil der Lösung

Idee:

- Zusätzlich zu automatisch auch manuell
- Analog zu Handfeuermelder
  - Für Sicherheitsvorfälle
  - Losgelöstes System

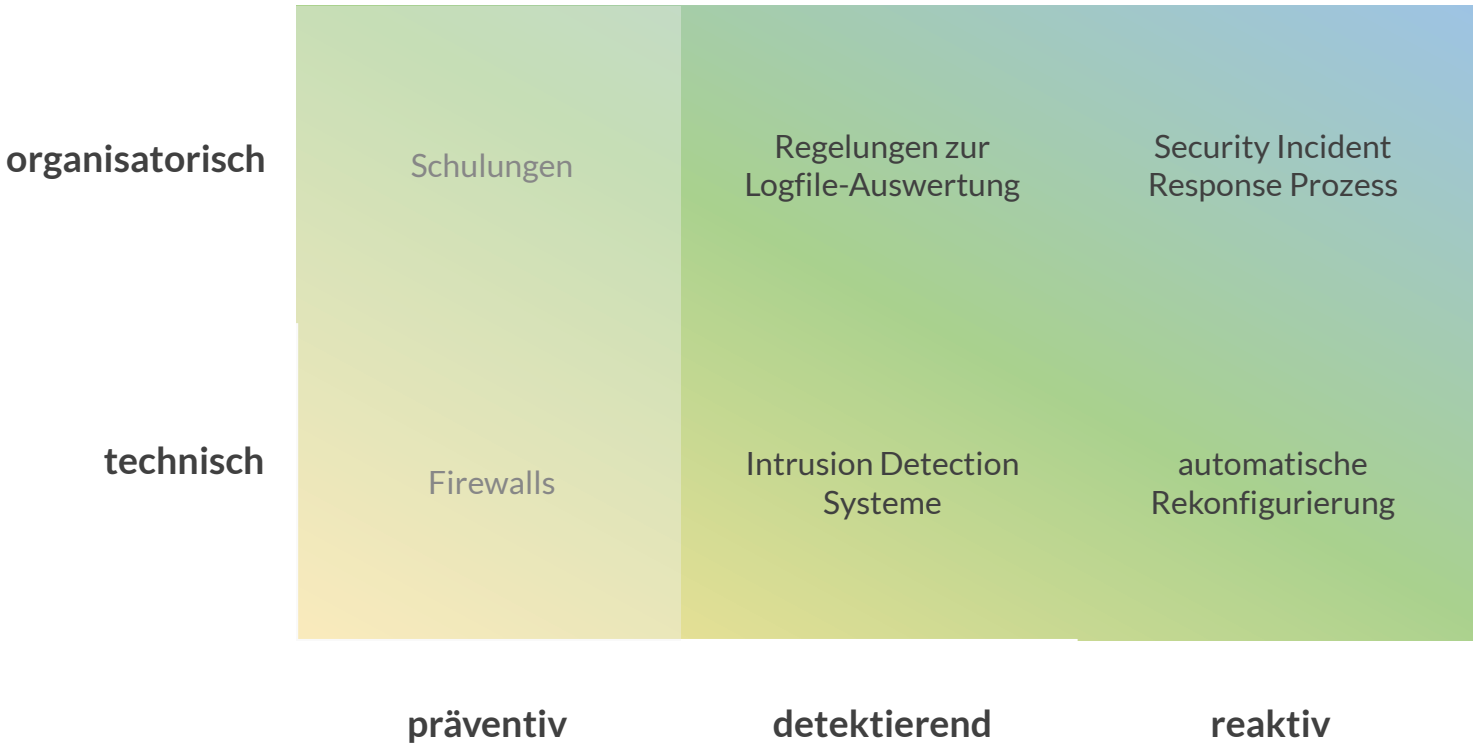
Quelle: https://www.baunetzwissen.de/imgs/1/5/0/3/2/6/7/bdf651731e74eca6.jpg

- Das Gjallarhorn
  - Keltische Mythologie
  - Benutzt von Heimdallr
    - Wächter der Brücke zwischen den Welten
  - Um vor Angreifern zu warnen

Quelle: https://www.deviantart.com/ethicallychallenged/art/Heimdallr-562229991

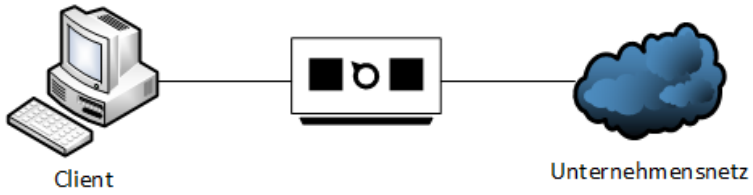
Idee:

Maßnahmen (Beispiele):

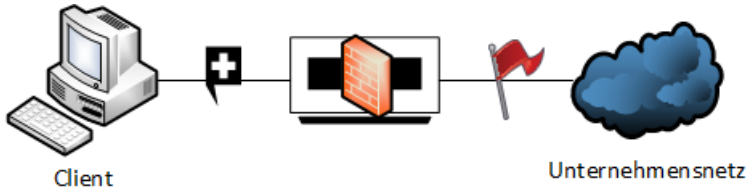


Idee

- Status „normal“



- Status „Meldung“

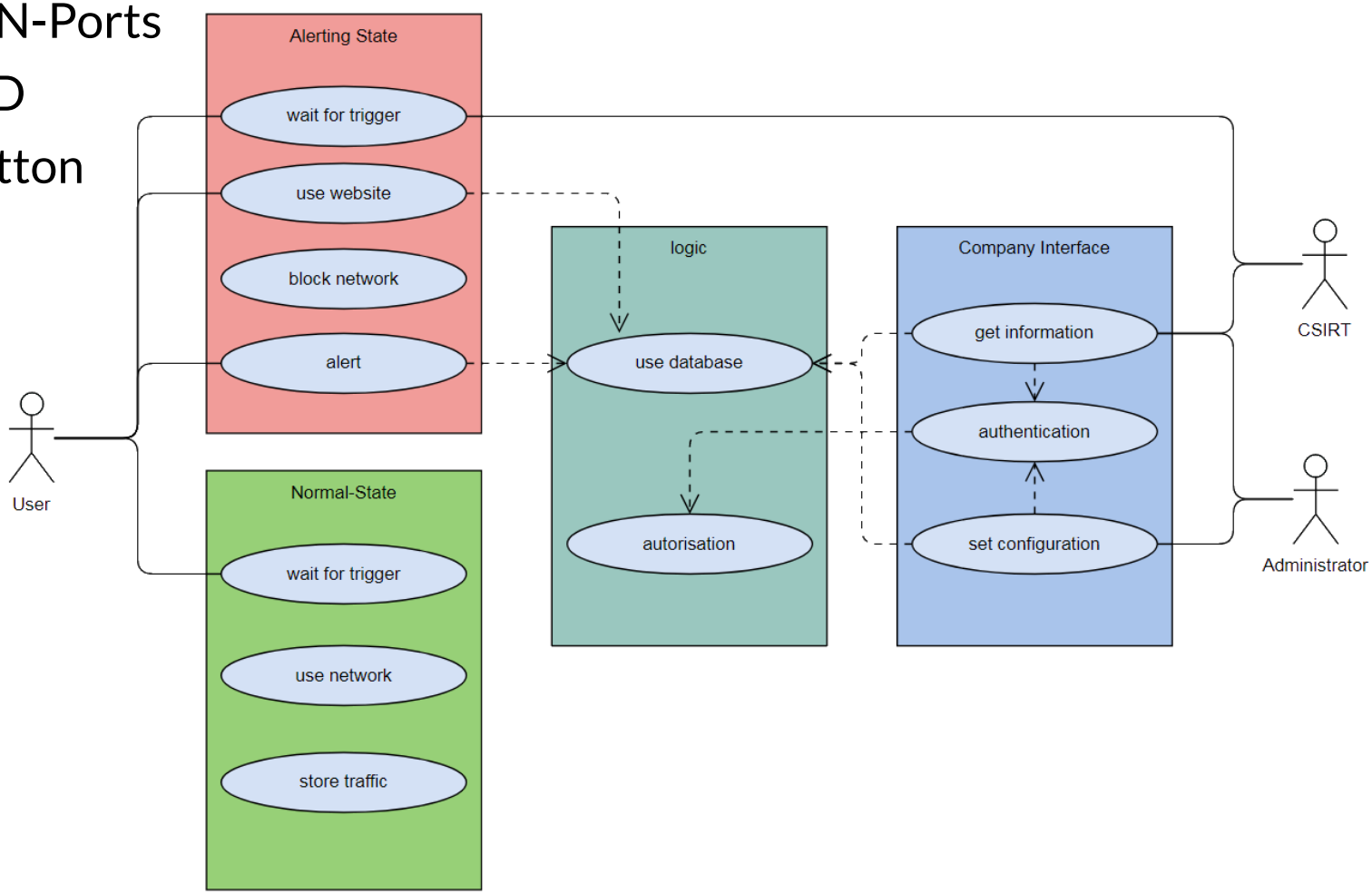


Von der Idee zum Konzept

- Abgleich mit etablierten Vorgehensmodellen
  - Idee ist damit kompatibel
- Anforderungsanalyse
  - funktional: Stakeholderanalyse
  - nichtfunktional: qualitative Anforderungen nach ISO/IEC 25010
    - Starker Fokus auf Security Anforderungen

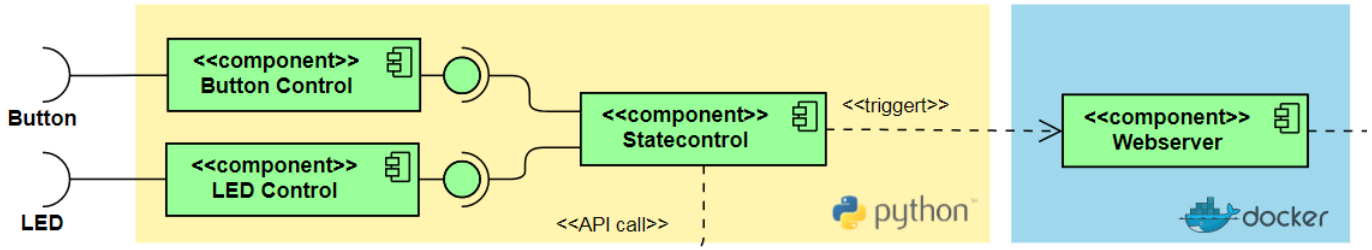
Grobdesign

- Singleboard Computer
  - 2 LAN-Ports
  - 1 LED
  - 1 Button



Konzept

User 1



Security Maßnahmen

- Allgemeine Systemhärtung
  - Rechte reduzieren
  - Netzwerkdienste deaktivieren
  - …
- Zusätzliche Systemhärtung
  - Vuls.io
  - Apparmor
  - Write xor Execute
  - SSH per default aus
  - Restriktive IPTables
  - Ein- u. Ausgabe sanitization / validation

MVP - Minimum Viable Product

- Orange pi R1H2
  - 2 LAN Ports (max 35 MB/s da USB2)
  - GPIO Pins für LED und Button
  - ARM Prozessor
  - Quadcore (1.5 GHz)
  - 256 MB DDR3
- ~25€

EOF

Vielen Dank!

Fragen?

rene.woelker@codecentric.de

(pgp fingerprint: 0xC7C07B20EA66060D)