

## **ibeco – „Private/Public Cloud“**

### **Datensicherheitskonzept**

- Zutrittskontrolle
  - o Elektronisches Zutrittskontrollsystem
  - o Sämtliche Zufahrten, Eingänge und Serverräume sind videoüberwacht
- Zugangskontrolle
  - o Bei Erstbezug oder einem temporären Techniker-Besuch beauftragter Serviceunternehmen muss vorab in der Administrationsoberfläche der Besuchstermin und die Zutrittsberechtigungen festgelegt werden.
  - o Mittels eines generierten Passworts erfolgt beim Service-Personal vor Ort die Authentifizierung und die Aushändigung des Transponderchips für den Schleusen-Zugang zum Rack. Der Aufenthalt wird dabei protokolliert und aufgenommenes Bildmaterial in der Administrationsoberfläche zur Kontrolle archiviert.
  - o Rechenzentrumsbetreiber und Mitarbeiter haben keinen logischen Zugriff auf das System (mehrfach Passwortgeschützt)
- Ein modernes Brandfrühsterkennungssystem ist direkt mit der Brandmeldezentrale der örtlichen Feuerwehr verbunden.
- Zugriffskontrolle
  - o Administrativen Zugriff auf die Private/Public Cloud haben ausschließlich Mitarbeiter der Fa. ibeco-Systems GmbH
  - o Kunden oder Mitarbeiter haben keinen Administrative Zugriff auf die Hosts der Private Cloud oder die Plattform
- Weitergabekontrolle
  - o Auf dem Private Cloud Cluster gespeicherte Daten werden in keiner Weise vom Auftraggeber an Dritte weitergegeben.
- Trennungskontrolle
  - o Aufgrund getrennter virtueller Maschinen (pro Kunde) ist eine Vermischung von Daten und Systemen nicht möglich. Die Daten und Systeme werden somit getrennt verarbeitet und gespeichert.
- Verfügbarkeitskontrolle
  - o Die unterbrechungsfreie Stromversorgung (USV) wird durch eine 15-minütige Batteriekapazität und Notstrom-Dieselaggregate garantiert.

Sämtliche USV-Anlagen sind dabei redundant ausgelegt.

- Die direkte freie Kühlung sorgt für eine umweltschonende Kühlung der IT-Hardware. Die Klimatisierung erfolgt über den Doppelboden.
  - Vielfach redundante Anbindungen, darunter an den größten deutschen Austauschknotten DE-CIX, sorgen für einen reibungslosen Datenaustausch
  - Das System ist redundant aufgesetzt, sodass auch ein vollkommener Ausfall des Rechenzentrums keine Auswirkungen auf die Verfügbarkeit der Daten, bzw. der Zustellung der E-Mails hat.
- Auftragskontrolle
    - Konfigurationsänderungen werden nur nach Weisung des Auftraggebers durchgeführt
    - Einzelweisung zur Auftragserledigung
    - Einzelanweisung zu zusätzlichen Sicherheitsmaßnahmen
  - Datengeheimnis
    - Beschäftigte des Auftragnehmers sind auf das Datengeheimnis verpflichtet
    - Kein Einsatz von Subunternehmern