Rollen und Sicherheit

Neue Rollen durch veränderte Arbeitsabläufe

Mit der Einrichtung einer zentralen Gebäudesteuerung verändern sich die Arbeitsabläufe im kommunalen Gebäudemanagement stark. Während einige Aufgabenfelder ersatzlos wegfallen und durch die Automationsebene übernommen werden, entstehen z.B. in der Verwaltung der Systeme ganz neue Aufgabenbereiche, die es zuvor nicht gab.

Mitarbeiter müssen in Steuerung, Überwachung und Verwaltung des Gebäudemanagementsystems eigebunden werden. Dies sollte anhand einer geplanten und strukturierten Rollenaufteilung geschehen, so dass alle Mitarbeiter ihre zugeteilten Aufgaben effizient erfüllen können und im System genau die Rechte haben, die dafür nötig sind. Arbeitsabläufe können damit sowohl flexibel als auch sehr effizient gestaltet werden. Eine Übergabe von Rechten von einer Person auf die andere, ein Entzug gewisser Rechte oder das erteilen von neuen Rechten ist schnell und unkompliziert möglich.

Um einen Überblick über wichtige Aufgabenbereiche in einem zentralisierten Gebäudemanagementsystem zu gewinnen, werden im Folgenden die wichtigsten Rollen in einem automatisierten, zentral gesteuerten Gebäude(-park) skizziert

Welche Rollen sind grundlegend sinnvoll?

Systemintegration (erstmaliges Setup)
→ kann externalisiert werden, aber eigene Leute zu integrieren ist sinnvoll

IT-Techniker oder externer Dienstleister, der das System aufbaut

Administration
auf Gesamtebene
auf Gebäudeebene

IT-Techniker, Gebäudemanager

Benutzer
Anwendungsebene (Nutzer haben i.d.R. kein Zugriff auf das System)
„SuperBenutzer“ zusätzlich definierbar

Nutzer der Gebäude; kommunale Mitarbeiter sowie Besucher

Controller
nur lesend zugreifend; Zugriff auf alle Variablen. Kann diese aber nicht ändern, Visualisierung, Berichte erstellen

Evtl. Finanzzuständige, Energiemanager, Klimaschutzmanager

Handwerkerzugang (lesend zugreifen; Energiemessstände kontrollieren, Aktoren- und Sensorenzustände einsehen und prüfen)
Gebäudeebene
Anwendungsbasiert

Handwerker und andere Dienstleister

Alarmierung = wer bekommt welche Alarmierungen
Gebäudebezogen (z.B. Hausmeister nur für Schule
Anwendungsbezogen (z.B. Brandmeister nur für Brandmelder im Stadtbereich)

Gebäudemanager, Sicherheitskräfte, Polizei, Feuerwehr

Sicherheit

Wichtig ist an dieser Stelle auch der Aspekt Sicherheit. Ein zentralisiertes und automatisiertes System bietet hier gewisse Vorteile aber auch neue Risiken: In digitalen Systemen reicht eine rein physische Zugangsbeschränkung nicht mehr aus, um die Systemsicherheit zu gewährleisten. Die Zugangs- und Zugriffsmöglichkeiten einzelner Mitarbeiter lassen sich dynamisch festlegen und können nicht ohne weiteres umgangen werden. Auch lassen sich einzelne Zugriffe erlauben oder sperren, ohne dass eine physische Änderung notwendig ist. Dies gilt umso mehr, wenn auch die Zutrittskontrolle Teil des Gebäudemanagements ist.

Grundlage für die Rechtevergabe sollte dabei immer ein Gruppen- und Rollenkonzept und keine individuellen Rechtezuweisungen sein. Sollte eine sicherheitsrelevante Fehlbedienung eingetreten sein, kann die Ursache schnell gefunden und die betreffenden Personen entsprechend informiert werden. Dies ist dies ist in einem manuell verwalteten Rechtesystem oftmals fehleranfällig und schwierig umzusetzen.

Zugriffe von außen

Um Zugriffe von außen zu vermeiden, sollten alle Systeme wie auch die hauseigene IT auf Servern installiert sein, die entsprechend abgeschottet sind und den Sicherheitsrichtlinien genügen. Grundsätzlich gilt hier erst einmal, alle Zugriffe von außen zu verhindern, und dann selektiv einzelne Zugriffe zu erlauben. Dies bietet einen deutlich höheren Sicherheitsstandard als der Versuch, ein offenes System selektiv abzuschotten.

Eine Leitlinie, die verbindlich für alle Kommunen ist, bietet hier das Dokument „Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der

Informationstechnik 2020“ [1]der Bundes- und Landesrechnungshöfe. Ebenso zu Rate zu ziehen ist die „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung 2018“[2] des IT-Planungsrates. Wenn diese gewissenhaft umgesetzt wird, werden Cyberattacken enorm erschwert.

Betriebssicherheit

Für kommunale Liegenschaften ist ein zuverlässiger Betrieb essenziell. Ein zentrales, automatisiertes System kann hierzu mit beitragen: Störungen können sehr schnell und zuverlässig erkannt und die Ursachen behoben werden. Grundlage dafür ist ein ausfallsicheres Backbone: Noch mehr als in der kommunalen IT ist auf Redundanz und Ausfallsicherheit zu achten. Auch muss sichergestellt werden, dass automatisierte Gebäude im Falle des Verlustes der Verbindung zur Zentrale autark funktionieren.

Auch sollten allgemeine Datennetze und Netze für die Gebäudeautomation getrennt sein, ideal ist eine physische Trennung, sollte dies nicht möglich sein, so ist zumindest eine Trennung in verschiedene virtuelle Netze (vLAN) zu realisieren.

Rollenaufteilung

- Wichtig: Rollen können auf verschiedenen Ebenen angelegt werden → favorisiert werden sollten die Rollen auf der oberen Ebenen zu definieren und dann auf die unteren Ebenen zu verteilen
- Wer kann die Rollen ausfüllen, welche Vertretungsregeln gibt es im Alternativfall?
- Matrix zur Rollenverteilung stellt DUH den Modellkommunen zur Verfügung
- Rollen werden dann im System einmal definiert → wichtige Aufgabe welche Personen stehen hier dahinter
- **Wichtig** im Rahmen der Rollenvergabe:
    - Individuelle personalisierte Accounts erstellen
    - Accounts anlegen = Aufgabe des Admins
    - Ermöglicht Transparenz bei Änderungen im System
    - Zur Sicherheits-Backup Accounts auf der Gebäudeebene spiegeln

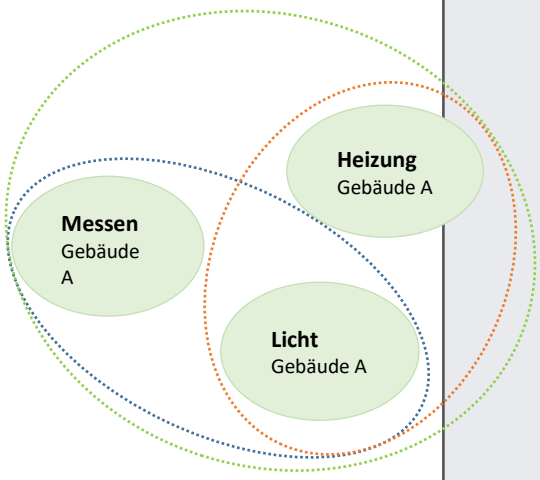

Abb.: Visualisierung Rollenzuordnung

[1] http://l.duh.de/vnah7
[2] http://l.duh.de/7gajm

- **Welche Rollen sind grundlegend sinnvoll:**
  - **Systemintegration** = erstmaliges Setup
    kann externalisiert werden, aber eigene Leute zu integrieren ist sinnvoll
  - **Administration**
    auf Gesamtebene
    auf Gebäudeebene
  - **Benutzer**
    Anwendungsebene (Nutzer haben i.d.R. kein Zugriff auf das System)
    „SuperBenutzer“ zusätzlich definierbar
  - **Controller** = weitreichende Rolle, aber nur lesend zugreifend; Zugriff auf alle Variablen, kann diese aber nicht ändern, Visualisierung, Berichte erstellen
  - **Handwerkerzugang** = lesend zugreifen; Energiemessstände kontrollieren, Aktoren- und Sensorenzustände einsehen und prüfen
    Gebäudeebene
    Anwendungsbasiert
  - **Alarmierung** = wer bekommt welche Alarmierungen
    Gebäudebezogen (z.B. Hausmeister nur für Schule
    Anwendungsbezogen (z.B. Brandmeister nur für Brandmelder im Stadtbereich)