**1. Wahrnehmung und Feststellung des Problems (deskriptive Ebene)**

**Ethisches Problem:**  
Das Hauptziel des Systems ist es, die Sicherheit und Effizienz in Rechenzentren zu erhöhen. Dabei entsteht jedoch ein Spannungsfeld zwischen **Sicherheit** und **Datenschutz**. Mögliche ethische Fragen sind:

* Wie wird sichergestellt, dass die erfassten Daten (z.B. Zutrittszeiten, Bewegungsprofile, Temperaturverläufe) nicht missbraucht werden?
* Werden die Nutzer (Kunden und Entwickler) ausreichend über die Art und den Umfang der Datensammlung informiert?
* Wie wird die Privatsphäre der Mitarbeiter und Kunden geschützt?
* Wie werden unbefugte Zugriffe erkannt und verhindert?
* Wie transparent ist das System in Bezug auf seine Überwachungsfunktionen?

**Zentrale Frage:**  
„Wie können wir maximale Sicherheit gewährleisten, ohne die Rechte und die Privatsphäre der Nutzer zu verletzen?“

**2. Situations- und Kontextanalyse (Vertiefung deskriptive Ebene)**

**Zeitlich:** Wann und wie oft greifen die Nutzer auf das System zu? (z.B. regelmäßig, im Notfall, 24/7 Überwachung)  
**Biografisch:** Gibt es unterschiedliche Nutzergruppen (Techniker, IT-Administratoren, Sicherheitskräfte)?  
**Personal:** Wer hat Zugang zu den erfassten Daten und wie sind die Zugriffsrechte verteilt?  
**Institutionell:** Gibt es besondere Vorschriften für Rechenzentren (z.B. DSGVO, ISO 27001)?  
**Kulturell:** Gibt es internationale Kunden mit unterschiedlichen Erwartungen an Datenschutz und Privatsphäre?

**3. Entwurf von mind. drei Handlungsmöglichkeiten**

1. **Maximale Transparenz und Kontrolle für den Kunden:**
   * Jeder Zugriff wird protokolliert und für den Kunden einsehbar gemacht.
   * Kunden können individuell festlegen, welche Daten erfasst werden dürfen.
   * Regelmäßige Audits und Penetrationstests zur Überprüfung der Systemsicherheit.
2. **Datensparsamkeit und Anonymisierung:**
   * Daten werden nur in aggregierter oder anonymisierter Form gespeichert, wenn möglich.
   * Strikte Zugriffsrechte und rollenbasierte Benutzerkonten.
   * Minimierung der erfassten Daten auf das absolut notwendige Maß.
3. **Technologische Schutzmaßnahmen:**
   * Verschlüsselung der Daten während der Übertragung (über MQTT) und Speicherung.
   * Multi-Faktor-Authentifizierung (MFA) für alle Nutzer.
   * Implementierung eines Alarmsystems bei ungewöhnlichen Zugriffsversuchen.

**4. Beurteilung der Handlungsmöglichkeiten**

|  |  |  |  |
| --- | --- | --- | --- |
| **Kriterium** | **Maximale Transparenz** | **Datensparsamkeit** | **Technologische Schutzmaßnahmen** |
| **Sicherheit** | Hoch | Mittel | Sehr hoch |
| **Privatsphäre** | Mittel | Sehr hoch | Hoch |
| **Nutzerfreundlichkeit** | Mittel | Hoch | Mittel |
| **Kosten** | Hoch | Mittel | Hoch |
| **Umsetzbarkeit** | Mittel | Hoch | Mittel |
| **Flexibilität** | Hoch | Mittel | Mittel |

**Empfohlene Option:**  
Nach Abwägung aller Kriterien scheint die Kombination aus **Datensparsamkeit** und **Technologischen Schutzmaßnahmen** die ethisch vertretbarste Lösung zu sein, da sie sowohl hohe Sicherheit als auch guten Datenschutz bietet, ohne die Benutzerfreundlichkeit stark zu beeinträchtigen.

**5. Ethische Entscheidung**

Wir empfehlen, den Fokus auf die Kombination aus **Datensparsamkeit** und **Technologischen Schutzmaßnahmen** zu legen. Dies ermöglicht eine hohe Sicherheit und Wahrung der Privatsphäre, während die Kosten und Komplexität im Rahmen bleiben. Ein solcher Ansatz stärkt das Vertrauen der Kunden und erfüllt wichtige Datenschutzanforderungen.

**6. Dokumentation, Rückblick und Überprüfung**

Regelmäßige Audits, Überwachung der Systeme und kontinuierliche Verbesserung der Sicherheitsprotokolle sind notwendig, um den ethischen Standards langfristig gerecht zu werden. Zudem sollten regelmäßige Schulungen und Informationskampagnen für alle Nutzer durchgeführt werden, um das Sicherheitsbewusstsein zu stärken.