

# Cloud-basierte Gebäudeautomation: Schutz für vertrauliche Daten

Die Digitalisierung bietet der Immobilienbranche Produkte und Dienstleistungen, die es Gebäude-Entwicklern und Betreibern ermöglicht, ihre Geschäfte auf vielfältige Weise auszubauen. Eine Schlüsseltechnologie ist dabei die Cloud. Sie erweitert produktive und profitable Nutzungsmöglichkeiten – und das rund um die Uhr und unabhängig von den zum Einsatz kommenden Geräten. Dabei rückt die Sicherheit dieser Produkte und Dienste und der darin verarbeiteten Daten in den Fokus aller Beteiligten.



Gelf de Reus,  
Technischer Support,  
Vertrieb Österreich,  
Priva Building  
Intelligence GmbH,  
Tönisvorst

## Warum die Cloud?

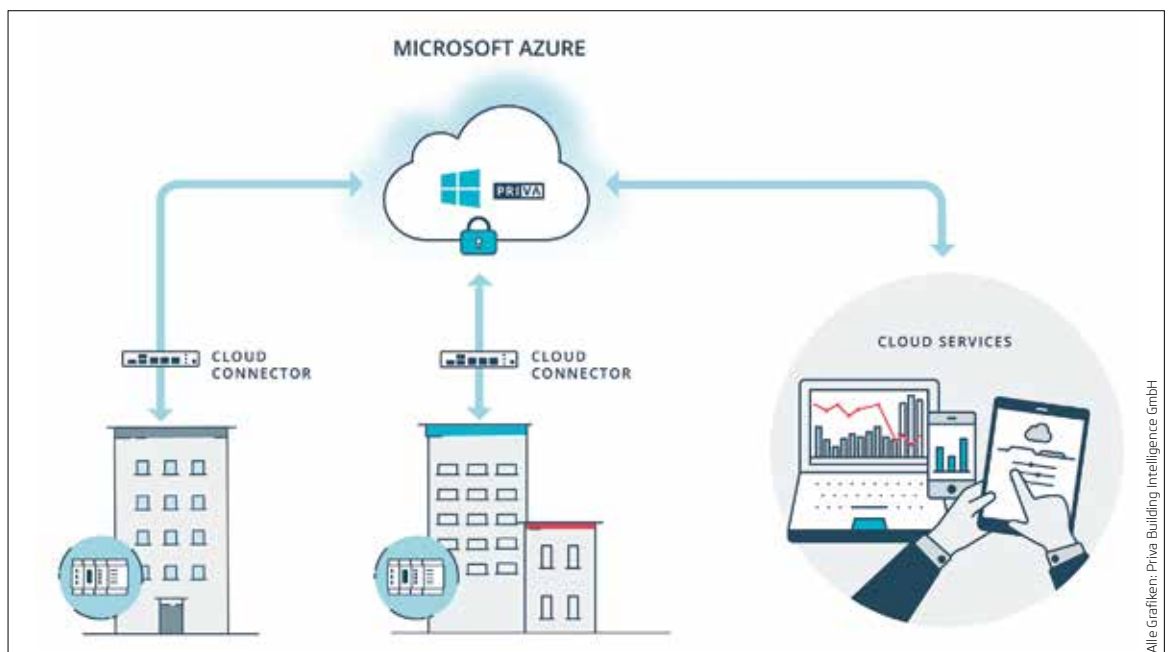
Für die Digitalisierung der Gebäude werden unterschiedliche Ansätze der Nutzung von Cloudtechnologie angeboten. Im Folgenden wird das Konzept vorgestellt, das Priva bei der Entwicklung ihrer Cloud-basierten Dienste verfolgt. Einblick wird gegeben in die

Schritte, die das Unternehmen unternommen hat, um Datensicherheit zu gewährleisten.

„Cloud“ bezeichnet die Technologie, die es Unternehmen ermöglicht, Datenspeicherung, Datenkommunikation und Rechenleistung zur Datenverarbeitung in das Internet auszulagern. Das Konzept dieser online verfügbaren IT-Struktur ist einfach: Anstatt eigene Rechenzentren einzurichten und zu pflegen, nutzen Unternehmen Online-Ressourcen – die Cloud –, um knappe interne IT-Infrastruktur strategisch auszulagern. Gebäudeeigentümern und Facility Managern ermöglicht die Cloud unter anderem den Fernzugriff auf Energieverbrauchs-, Nutzungs- und Prozessdaten. Darüber hinaus bietet sie eine umfassende Datenintelligenz, auf deren Basis große Informationsmengen verarbeitet, analysiert und gespeichert werden können.

Das mittels der Gebäudeautomation angestrebte kontinuierliche Erreichen und Optimieren eines Raumklimas für produktivitätssteigernden Komfort ist ein komplexer Prozess, der bisher mit großem Aufwand verbunden war. Vor diesem Hintergrund folgt das Konzept der Prämisse, dass Komfort mit so wenig Mühen und Arbeit wie möglich erreicht werden muss. Jeder Nutzer soll von der verwendeten Technologie mit minimalem Aufwand und Vorwissen profitieren.

Die Lösung besteht darin, Produkte, Systeme und Lösungen weitestgehend in Cloud-basierte Dienste zu verwandeln. Mit der Cloud verbunden arbeitende Software ermöglicht es, Gebäudeeigentümern und Facility Managern u. a. Fernüberwachung der Klimatisierungs-Systeme zu realisieren, die Anlagen-Effektivität standortübergreifend zu vergleichen, Energiekosten zu bewerten, Warmmel-



Unterschiedliche Gebäudeautomations-systeme lassen sich über die Cloud auf einer Bedienebene visualisieren.



dungen zu verwalten und Wartungsarbeiten durchzuführen, bevor Störungen auftreten.

Die Cloud im Automationseinsatz stellt Rechenleistung für die Verarbeitung der unterschiedlichen Daten aus verteilten Quellen zur Verfügung, macht diese Daten von jedem Ort aus zugänglich und erleichtert auf diese Weise kontinuierlich die Zusammenarbeit aller für das „Funktionieren“ einer Immobilie verantwortlichen Personen. Kurz gesagt: Cloud-basierte Lösungen haben das Potenzial, die richtigen Personen rund um die Uhr mit den richtigen Informationen zu versorgen.

### Sicherheit und Compliance auf der Cloud-Plattform

Priva hat sich dazu entschieden, ihre Dienste auf der Cloud-Plattform Azure von Microsoft zu entwickeln. Hintergrund sind zum einen die umfangreichen Sicherheitsmaßnahmen, die Microsoft einsetzt, zum anderen die Funktionalität der Standardkomponenten der Azure Cloud Computing-Plattform. Während die Experten von Microsoft die Sicherheit von Diensten und Daten gewährleisten, können sich die Entwickler auf die eigentliche Entwicklung von Cloud-Diensten konzentrieren. Diese „Arbeitsteilung“ ist sinnvoll, denn die Sicherheit von Software zu gewährleisten, ist eine schier unüberschaubare Aufgabe. Sie erfordert spezielles Know-how und einen großen Aufwand. Als führender Plattformanbieter verfügt Microsoft über die notwendigen Ressourcen, in die Sicherheit von Cloud Computing zu investieren. Was sich auszahlt: Azure erfüllt mehr als 75 lokale, regionale und weltweite Standards. Mit der Einhaltung von Normen wie ISO/IEC 27018 und DSGVO-Gesetzgebung stellt Microsoft eine Infrastruktur zur Verfügung, die verarbeitete Daten umfassend schützt. Insgesamt wird ein Sicherheits- und Compliance-Niveau erreicht, das kein einzelnes Unternehmen mit seiner eigenen Informations- und Kommunikations-Abteilung erreichen könnte.

### Daten-Sicherheit für digitale Gebäude

Im Detail wird die Sicherheit der Cloud-Dienste mittels aufeinander abgestimmter Komponenten erreicht. Alles startet mit der klassischen Gebäudeautomation: Die Automation besteht aus dem Netzwerk der zum Einsatz kommenden einzelnen Controller, die das gesamte Klima eines Gebäudes steuern. Oft sind Gebäudeautomations-Controller datentechnisch nicht ausreichend gesichert. Dazu kommt, dass die wesentlichen Steuerungs-Protokolle der Gebäudeautomation, die auf diesen Controllern „laufen“, nur wenige Möglichkeiten zur Daten-Verschlüs-

Pioneering for You

wilo



NEU

### Geben Sie Keimen keine Chance. Mit Wilo-ThermoDes.

Mit dem Kauf einer Druckerhöhungsanlagen von Wilo sind Sie auf der sicheren Seite. Alle Anlagen werden vor Auslieferung zusätzlich zur chemischen Desinfektion auch thermisch desinfiziert. Betreiber und Verarbeiter, die auch nachträgliche Verkeimungen, z. B. bei Transport oder Lagerung, ausschließen wollen, können auf Wilo-ThermoDes mobil zurückgreifen.

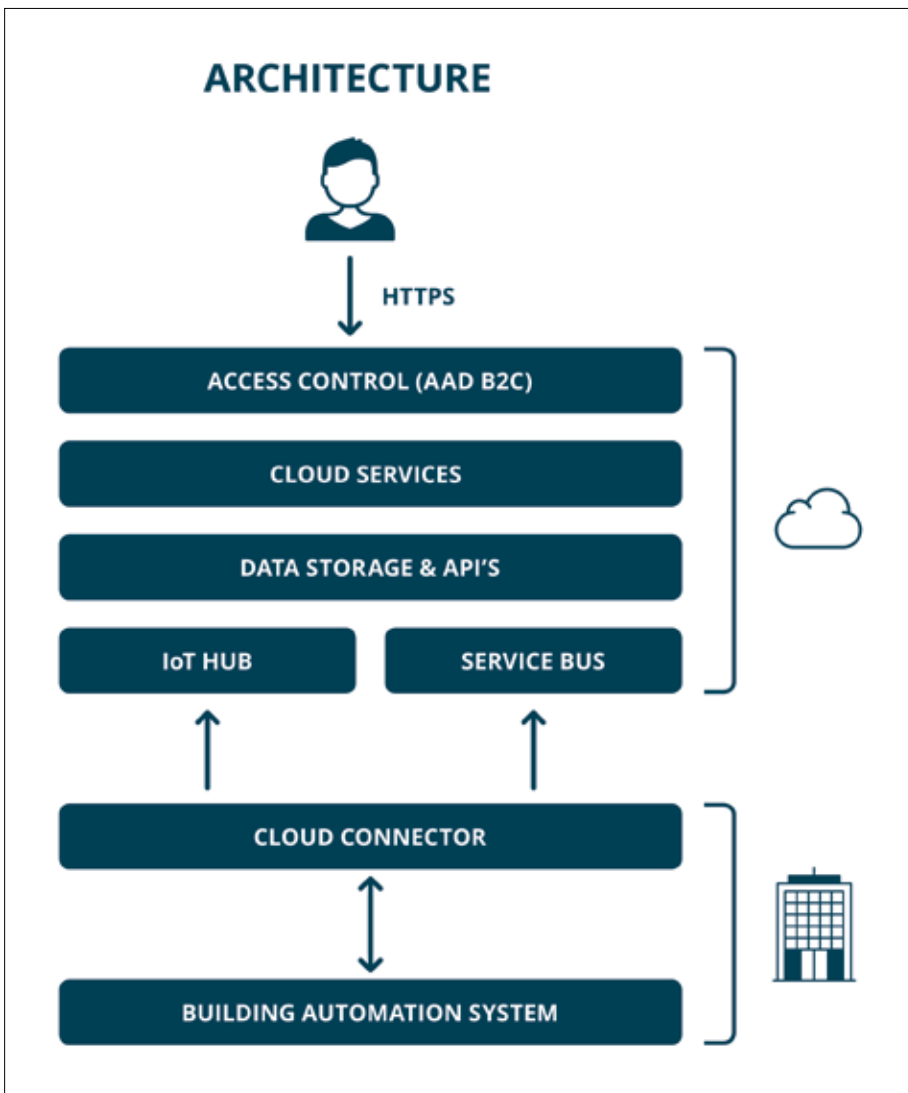
#### Ihre Vorteile:

- Echtes Hygiene-Plus dank Wilo-ThermoDes Verfahren
- Präventive Hygienemaßnahme dank doppelstufiger Desinfektion aller Druckerhöhungsanlagen im Produktionswerk
- Einhaltung der mikrobiologischen Anforderungen der Trinkwasserverordnung
- Maximale Sicherheit und Flexibilität auch am Einbauort dank Wilo-ThermoDes mobil
- Verfahren bestätigt vom unabhängigen Rheinisch-Westfälischen Institut für Wasser mit Schwerpunkt auf der Eliminierung von Pseudomonas aeruginosa (PSA)
- Garantierte Sicherheit im Zweifelsfall

[www.wilo.de/thermodes](http://www.wilo.de/thermodes)



Künstliche Intelligenz kann über „digitale Zwillinge“ das Klima in einem Gebäude autonom steuern.



Architektur von Cloud-Diensten mit Cloud-Connector als sicheres Interface

selung bieten, beispielsweise BACnet. Gebäudeautomations-Systeme sollten deshalb niemals mit dem Internet direkt vernetzt werden. Sie benötigen stets ein spezielles technisches Netzwerk, das Sicherheit dadurch garantiert, dass ein direkter Zugang von außen verhindert wird.

Eine Möglichkeit für einen sicheren Cloud-Zugang ist ein Cloud-Connector. Dieser fungiert als Hardware-Plattform, die die für Cloud-Dienste erforderlichen Daten aus dem Gebäudeautomations-System sammelt und in die Cloud überträgt.

Um Cloud-Dienste nutzen zu können, muss das Controller-System eine Verbindung mit dem Internet herstellen, wobei das System keinen direkten Online-Zugang haben darf. In diesem Zusammenhang hat der Cloud-Connector die wichtige Funktion, die notwendige sichere Schnittstelle zwischen dem Controller-System und dem Internet bereitzustellen. Zu diesem Zweck ist der Cloud-Connector mit zwei separaten Netzwerkkarten ausgestattet. Auf diese Weise wird das Automations-Netzwerk physisch komplett vom Internet trennbar und das Controller-System vor Zugriff von außen geschützt.

Darüber hinaus ist es wichtig, dass der Cloud-Connector gesichert mit der Cloud kommuniziert. Deshalb verfügt er lediglich über ausgehende Verbindungen und unterhält keine eingehenden Verbindungen. Kommunikation zwischen dem Gebäude und der Außenwelt wird ausschließlich vom Cloud-Connector selbst initiiert. Das Ergebnis ist, dass aus der Richtung des Internets gedacht, der Connector gar nicht existiert. Und was nicht existiert, kann auch nicht angegriffen oder gehackt werden.

Wenn der Cloud-Connector seine selbst-initiierte Verbindung zur Cloud herstellt, stehen wiederum Sicherheits-Anforderungen im Fokus: Die Dienste nutzen den IoT-Hub sowie den Service-Bus von Microsoft Azure. Alle Daten, die in die Cloud übertragen werden, sind durch Verschlüsselung gesichert.

### Fazit

Datensicherheit von Cloud-Diensten ist ein wichtiges Merkmal, das bei der Entwicklung der einzelnen Systembausteine von Anfang an zu konzipieren und zu integrieren ist. Das gilt am Ende auch für die Nutzung dieser Dienste. Zum Schutz vor unbefugtem Zugriff müssen sich die Nutzer von Diensten authentifizieren. Hierzu kommt ein Azure Cloud-Identitätsdienst für Business-To-Consumer-Apps zum Einsatz. Darüber hinaus erfolgt jegliche Kommunikation der Nutzer ausschließlich über das „abhörsichere“ HTTPS-Protokoll. ◀