



GEBÄUDESYSTEMTECHNIK

# Gebäudeautomation 2026: GEG, Daten und Cybersecurity als Treiber der Zukunft

- ▶ Einordnung technologischer und sicherheitsrelevanter Entwicklungen im Bereich der Gebäudeautomation

tab FACHFORUM

ZUKUNFT DER  
GEBÄUDEAUTOMATION 2026

- ▶ Einfach Vertrauen einbauen.

**WILDEBOER**

# Inhaltsverzeichnis

GEG, Daten und Cybersecurity als Treiber der Zukunft

## Inhaltsverzeichnis

<b>1</b>	<b>Begrüßung</b>	<b>3</b>
<b>2</b>	<b>Vorwort</b>	<b>4</b>
2.1	Vorstellung.....	4
<b>3</b>	<b>Rahmenbedingungen des Gebäudebetriebs</b>	<b>5</b>
<b>4</b>	<b>Zielgrößen im Gebäudebetrieb</b>	<b>6</b>
4.1	Technologieeinsatz im Gebäudebetrieb steigt.....	7
4.2	Wie wird Performance im Gebäudebetrieb bestimmt.....	8
<b>5</b>	<b>Rahmenbedingung Energieabhängigkeit</b>	<b>9</b>
5.1	Energieverbrauch im Gebäudebetrieb.....	9
<b>6</b>	<b>Rahmenbedingung Klimaschutz</b>	<b>10</b>
<b>7</b>	<b>Kostenentwicklung im Gebäudebetrieb</b>	<b>11</b>
7.1	Strategische Bedeutung für den Gebäudebetrieb.....	12
7.2	Energieeffizienz als strategischer Faktor.....	13
<b>8</b>	<b>Rahmenbedingung Regulatorik</b>	<b>14</b>
<b>9</b>	<b>Im Gebäudebetrieb entsteht doppelter Handlungsdruck</b>	<b>15</b>
<b>10</b>	<b>Datenbasierter Gebäudebetrieb</b>	<b>16</b>
<b>11</b>	<b>Praxisbeispiel Gebäudebetrieb</b>	<b>17</b>
11.1	Beispiel Volumenstromregelung.....	18
<b>12</b>	<b>Rahmenbedingung Cybersecurity</b>	<b>20</b>
12.1	OT wird zum Angriffsziel.....	21
12.2	Cybersecurity ist systemisch geregelt.....	22
12.3	Sichere Produkte sind Voraussetzung.....	23
12.4	Achtung bei Produkten ohne Updatefähigkeit.....	24
12.5	Sicherheit entsteht im Betrieb.....	25
12.6	Schwachstellenmanagement im Gebäudebetrieb.....	26
12.7	Praxisbeispiel Cyberangriff.....	27
<b>13</b>	<b>Leitlinien des Gebäudebetriebs</b>	<b>28</b>
<b>14</b>	<b>Produkthinweis</b>	<b>29</b>
<b>15</b>	<b>Whitepaper</b>	<b>30</b>
15.1	Whitepaper zum Vortrag.....	30
<b>16</b>	<b>Abschluss</b>	<b>31</b>

### 1 Begrüßung



#### Abstract

Die Rahmenbedingungen im Gebäudebetrieb verändern sich grundlegend. Steigende Anforderungen und zunehmende **Komplexität** erhöhen den Handlungsdruck.

Der Gebäudebetrieb wird durch drei miteinander verknüpfte Zielgrößen bestimmt:

- **Betriebssicherheit,**
- **Energieeffizienz** und
- **Komfort.**

Ihre Wechselwirkungen bestimmen die **Performance**. Sie ist der zentrale Bewertungsmaßstab für die Qualität des Gebäudebetriebs und Grundlage für dessen **Wirtschaftlichkeit**.

Mit steigender Technologiedichte wachsen Funktionsumfang und Vernetzung. Gleichzeitig steigt die Komplexität der Systeme und ihres Zusammenwirkens.

Mehr Technologie führt nicht automatisch zu besserer Performance. Systeme benötigen selbst Energie und erhöhen den Integrationsaufwand. Ohne ein abgestimmtes Zusammenwirken können erwartete Verbesserungen teilweise oder vollständig ausbleiben.

Komplexität wird damit zu einem eigenständigen Einflussfaktor. Ihre **Beherrschbarkeit** entscheidet über die erreichbare Performance.

Entscheidend ist nicht der Technologieeinsatz, sondern die damit erreichte Performance.

## 2 Vorwort



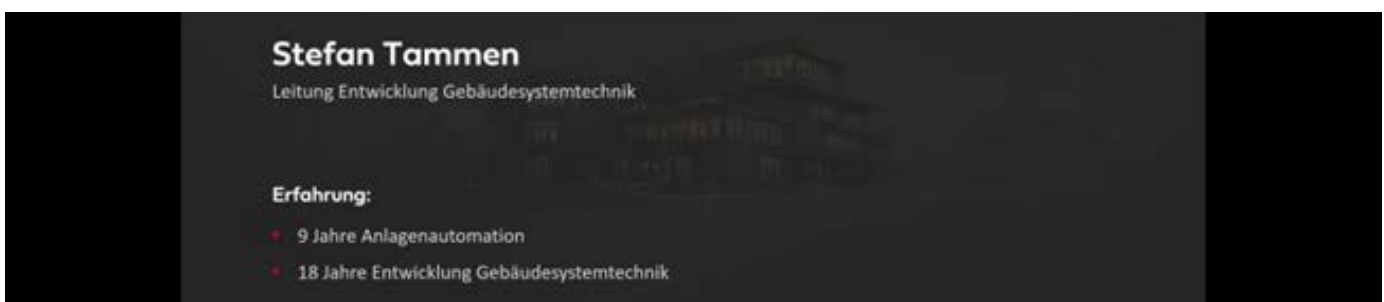
Medial wird Gebäudeautomation heute häufig auf Energieeffizienz und CO<sub>2</sub>-Reduzierung reduziert. Diese verkürzte Betrachtung wird weder der tatsächlichen Rolle der Gebäudeautomation noch den Anforderungen an einen performanten Gebäudebetrieb gerecht.

Ein performanter Gebäudebetrieb wird durch das Zusammenwirken mehrerer Zielgrößen bestimmt.

Die zentrale Frage lautet daher:



### 2.1 Vorstellung



Bevor auf die Zielgrößen im Gebäudebetrieb eingegangen wird, ist zunächst eine Einordnung der aktuellen Rahmenbedingungen erforderlich.

# Rahmenbedingungen des Gebäudebetriebs

GEG, Daten und Cybersecurity als Treiber der Zukunft

## 3 Rahmenbedingungen des Gebäudebetriebs



Die Rahmenbedingungen im Gebäudebetrieb haben sich deutlich verändert. Digitalisierung ist die Voraussetzung, um Systeme messbar, steuerbar und automatisierbar zu machen.

Gleichzeitig steigt mit der Vernetzung die Systemkomplexität. Die zunehmende Anzahl vernetzter Geräte, insbesondere im IoT- und OT-Umfeld, führt zu neuen Cyberrisiken. Energieabhängigkeiten führen zu Unsicherheiten bei Verfügbarkeit und Preisen. Diese werden durch geopolitische Entwicklungen zusätzlich verstärkt.

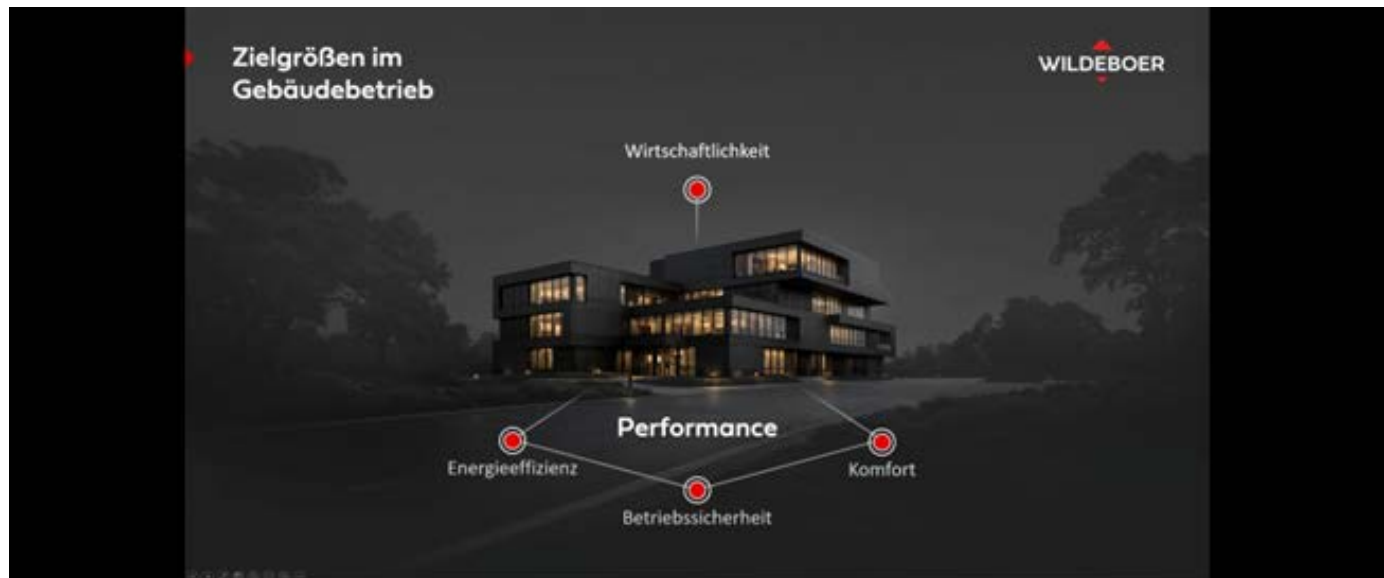
Klimaziele bestehen seit dem Pariser Klimaabkommen und werden regelmäßig verfehlt.

Diese Entwicklungen führen auf europäischer und nationaler Ebene zu einer zunehmenden regulatorischen Verdichtung, insbesondere in den Bereichen Energieeffizienz, Digitalisierung, Datenverfügbarkeit und Cybersecurity.

Hinzu kommt der Fachkräftemangel. In Deutschland fehlen aktuell rund 148.500 MINT-Fachkräfte. Dies wirkt sich über den gesamten Lebenszyklus von Gebäuden aus.

Diese Rahmenbedingungen wirken gleichzeitig und beeinflussen die Zielgrößen im Gebäudebetrieb.

## 4 Zielgrößen im Gebäudebetrieb



Der Gebäudebetrieb wird durch mehrere zentrale Zielgrößen bestimmt.

Die Betriebssicherheit bildet die Grundlage für einen stabilen Betrieb. Sie umfasst funktionale Sicherheit, Cybersicherheit und Verfügbarkeit. Verfügbarkeit wird dabei bewusst breiter gefasst und schließt Betrieb, Wartung und Instandhaltung ein.

Komfort beschreibt die Qualität der Nutzungsbedingungen im Gebäude. Er umfasst Funktionalität, Usability, User Experience, Raumluftqualität sowie die Behaglichkeit.

Energieeffizienz beschreibt den Energieeinsatz im Verhältnis zur bereitgestellten Funktion des Gebäudes. Ziel ist es, die Anforderungen an den Gebäudebetrieb mit minimalem Energieeinsatz zu erfüllen, ohne Komfort und Betriebssicherheit zu beeinträchtigen.

Die Performance ergibt sich aus dem abgestimmten Zusammenwirken dieser Zielgrößen im Betrieb.

Unter Einwirkung der Rahmenbedingungen bestimmt die Performance die Wirtschaftlichkeit des Gebäudebetriebs.

## 4.1 Technologieeinsatz im Gebäudebetrieb steigt



Zur Erreichung dieser Performance ist ein zunehmender Technologieeinsatz erforderlich. Die daraus entstehenden Daten bilden die Grundlage für die Digitalisierung im Gebäudebetrieb.

Mehr Technologie führt nicht automatisch zu besserer Performance. Sie erhöht die systemische Komplexität und damit die Anforderungen an die Beherrschung der Systeme.

Diese Komplexität wird durch die bestehenden Rahmenbedingungen zusätzlich verstärkt. Die sichere und wirtschaftliche Erreichung der Zielgrößen wird dadurch zunehmend herausfordernd.

Die zentrale Frage lautet:

Wie kann die Performance im Gebäudebetrieb unter diesen Bedingungen eindeutig und nachvollziehbar bestimmt werden?

## 4.2 Wie wird Performance im Gebäudebetrieb bestimmt



Entscheidend ist nicht die Planung allein, sondern das, was im Betrieb erreicht wird.

Jede Zielgröße hat im Betrieb eine konkrete und messbare Ausprägung. Energieeffizienz, Betriebssicherheit, Komfort und Wirtschaftlichkeit müssen im Betrieb erfüllt werden.

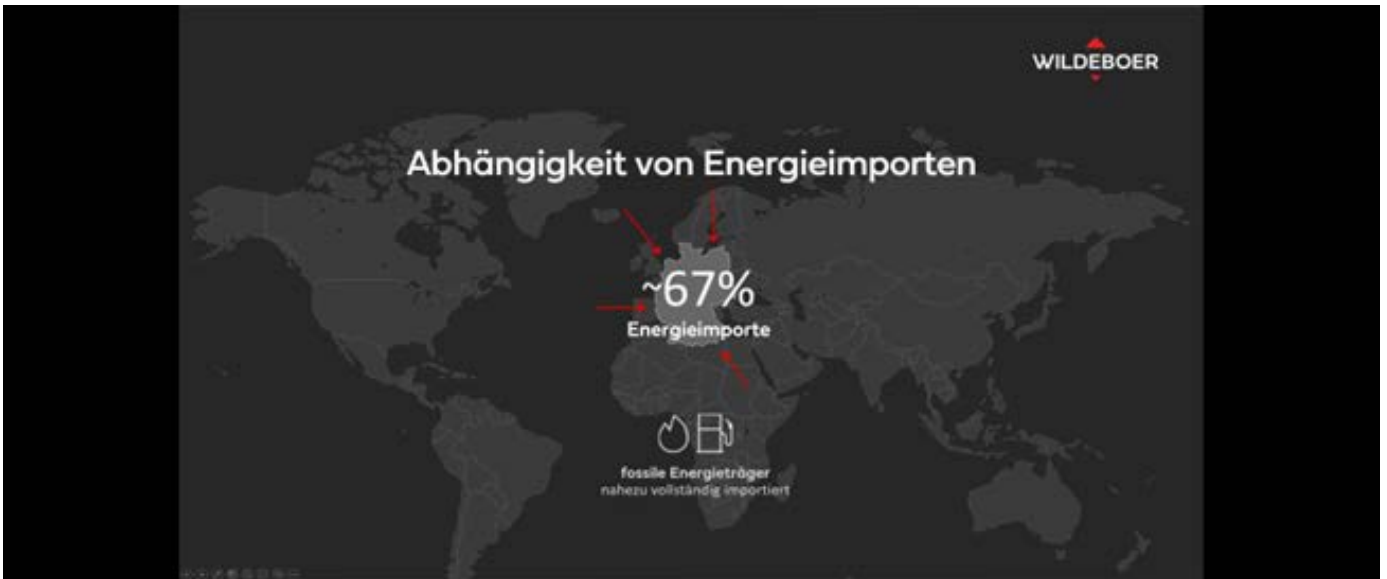
Die Zielgrößen können dabei nicht gleichzeitig optimal erreicht werden. Die Performance ergibt sich aus ihrem Zusammenwirken.

Wird die zunehmende systemische Komplexität unter den gegebenen Rahmenbedingungen nicht beherrscht, kann der steigende Technologieeinsatz zu Rebound-Effekten führen und die angestrebte Verbesserung der Zielgrößen konterkarieren.



Vor diesem Hintergrund kommt einer Zielgröße eine besondere strategische Bedeutung zu: der Energieeffizienz.

## 5 Rahmenbedingung Energieabhängigkeit



Ein wesentlicher Einflussfaktor im Gebäudebetrieb ist die Abhängigkeit von Energie. Deutschland ist in hohem Maß auf Energieimporte angewiesen, mit einem Anteil von rund 67 %.

Energiebedarf bedeutet damit immer auch Abhängigkeit von externen Märkten. Diese Abhängigkeit betrifft Preise, Verfügbarkeit und wirtschaftliche Rahmenbedingungen. Insbesondere bei fossilen Energieträgern besteht nahezu keine Eigenversorgung.

Vor diesem Hintergrund kommt dem Gebäudesektor eine besondere Bedeutung zu, da er einen erheblichen Anteil am Energiebedarf in Deutschland hat.

### 5.1 Energieverbrauch im Gebäudebetrieb



Der Gebäudesektor hat mit rund 43 % den größten Anteil am Energiebedarf in Deutschland. Er umfasst sowohl den Wohnungsbau als auch den Nichtwohnungsbau.

Damit liegt der größte Hebel zur Reduktion von Energiebedarf und Abhängigkeit im Gebäudesektor.

## 6 Rahmenbedingung Klimaschutz



Das Klimaschutzgesetz definiert einen Emissionspfad für den Gebäudesektor mit verbindlichen Zielwerten. Die Emissionsprojektionen zeigen die erwartete tatsächliche Entwicklung, die über diesem Zielpfad liegt.

Die Abweichung zwischen Ziel und Projektion setzt sich über die Jahre fort und summiert sich.

Bis 2030 ergibt sich daraus eine kumulierte Zielverfehlung von rund 110 Millionen Tonnen CO<sub>2</sub>-Äquivalenten.

Diese Abweichung bleibt nicht ohne Konsequenzen.



## 7 Kostenentwicklung im Gebäudebetrieb



Die Abweichung hat direkte Auswirkungen auf die Kostenstruktur im Gebäudebetrieb.

Kosten entstehen heute nicht mehr aus einem einzelnen Faktor, sondern aus mehreren gleichzeitig wirkenden Mechanismen. Zentrale Treiber sind die CO<sub>2</sub>-Bepreisung, steigende Netzentgelte und der Energiemix.

Die CO<sub>2</sub>-Bepreisung führt dazu, dass Emissionen unmittelbar zu Kosten werden. Gleichzeitig steigen die Netzentgelte infolge struktureller Veränderungen im Energiesystem. Die Infrastrukturkosten verteilen sich auf weniger Abnehmer und erhöhen die Belastung.

Das Preisniveau wird durch den Energiemix beeinflusst.

Gleichzeitig sind diese kostenbestimmenden Faktoren insgesamt durch eine hohe Volatilität geprägt.

Diese Faktoren wirken gleichzeitig, verstärken sich gegenseitig und werden überwiegend durch externe Entwicklungen bestimmt.



## 7.1 Strategische Bedeutung für den Gebäudebetrieb



Kosten entstehen heute überwiegend im Markt. CO<sub>2</sub>-Bepreisung, Energiepreise, Netzentgelte und Energieabhängigkeiten wirken gleichzeitig. Diese Faktoren sind volatil, nur begrenzt beeinflussbar und wirken direkt auf die Wirtschaftlichkeit.

Die Auswirkungen lassen sich am Beispiel der Netzentgelte verdeutlichen: Ausgehend von rund 63.000 Euro führen steigende Netzentgelte zu erheblichen Mehrkosten. Eine Studie des Fraunhofer-Institut für Fertigungstechnik und Angewandte Materialforschung IFAM zeigen, dass perspektivisch eine Vermehrfachung der Netzentgelte bis zum Faktor 10 möglich ist. Bereits bei einer Verfünffachung ergibt sich eine zusätzliche Belastung von rund 250.000 Euro. Bei einer typischen Produktmarge von 5 Prozent entspricht dies einem notwendigen zusätzlichen Umsatz von etwa 5 Millionen Euro.

Der Energiemix beeinflusst die Kostenstruktur direkt. Mit der Umstellung auf erneuerbare Energien sowie alternative Energieträger wie Biomethan oder synthetische Gase steigen die spezifischen Energiekosten. Gleichzeitig führen begrenzte Verfügbarkeiten und der erforderliche Ausbau von Infrastruktur und Versorgungssystemen zu zusätzlichen Systemkosten

(vgl. Klimaschutz- und Energieagentur Niedersachsen, Eckpunktepapier „Grüne Gase und Fernwärme“).

Auch die CO<sub>2</sub>-Bepreisung wirkt direkt auf die Kosten. Im nationalen Brennstoffemissionshandel (BEHG) gilt für das Jahr 2026 ein gesetzlich festgelegter Preiskorridor von 55 bis 65 Euro pro Tonne CO<sub>2</sub>. Mit der Einführung des europäischen Emissionshandels (ETS II) ab 2027/2028 ist mit einer deutlichen Dynamisierung zu rechnen. Perspektivisch werden bis 2030 Preisniveaus zwischen 120 und 200 Euro pro Tonne CO<sub>2</sub> erwartet.

Energieabhängigkeiten führen zu Unsicherheiten bei Verfügbarkeit und Preisen, die durch geopolitische Entwicklungen zusätzlich verstärkt werden.

Die wirtschaftliche Wirkung ist eindeutig: Kosten werden weitergegeben oder die Rendite sinkt. Die Weitergabe der CO<sub>2</sub>-Kosten ist jedoch durch das CO<sub>2</sub>-Kostenaufteilungsgesetz (CO<sub>2</sub>KostAufG) stufenweise begrenzt. Bei energetisch schlechten Gebäuden verbleiben bis zu 95 % der CO<sub>2</sub>-Kosten beim Eigentümer.

Der Markt selbst ist nicht beeinflussbar. Der Einfluss im Gebäudebetrieb liegt im Energiebedarf.

Dieser wird durch zwei zentrale Stellgrößen bestimmt: Energieeffizienz und Energieform.

Hier liegt der entscheidende Ansatzpunkt.

Nur Effizienz und Energieform  
reduzieren die Kostenwirkung und Risiken  
des Marktes.

# Kostenentwicklung im Gebäudebetrieb

GEG, Daten und Cybersecurity als Treiber der Zukunft

## 7.2 Energieeffizienz als strategischer Faktor



Aus dem Energiebedarf im Gebäudebetrieb und den damit verbundenen Abhängigkeiten ergibt sich eine direkte Wirkung auf Energiekosten, Versorgungssicherheit und externe Abhängigkeiten.

Diese Faktoren bestimmen die wirtschaftliche Resilienz des Gebäudebetriebs.

Da sich diese Abhängigkeiten nicht kurzfristig auflösen lassen, wird Energieeffizienz zu einem zentralen Enabler für einen resilienten Gebäudebetrieb.



## 8 Rahmenbedingung Regulatorik



Mit der EPBD werden die Anforderungen an den Gebäudebetrieb verbindlich definiert.

Der Fokus verschiebt sich stärker vom geplanten Zustand hin zur Bewertung und Überprüfung im realen Betrieb. Neben dem berechneten Zustand gewinnt der im Betrieb gemessene Zustand zunehmend an Bedeutung.

Zentrale Voraussetzung ist ein kontinuierliches Monitoring von Energieverbräuchen und Anlagenzuständen. Dafür müssen Daten verfügbar und transparent sein. Gleichzeitig ist Interoperabilität der Systeme erforderlich.

Diese Voraussetzungen ermöglichen den Nachweis im Betrieb und bilden die Grundlage für die Steuerbarkeit, auch im Zusammenspiel mit dem Energiesystem.

Ein Beispiel ist die lastabhängige Nutzung von Speichern im Zusammenspiel mit Photovoltaik, um Lastspitzen zu vermeiden, Kosten zu reduzieren und das Versorgungsnetz zu entlasten.

Diese Anforderungen ergeben sich aus dem regulatorischen Rahmen und den damit verbundenen Nachweis- und Betriebsanforderungen.

Ohne Monitoring, transparente Daten und Interoperabilität ist ein belastbarer Nachweis und eine gezielte Steuerung im Gebäudebetrieb nur eingeschränkt möglich.



# Im Gebäudebetrieb entsteht doppelter Handlungsdruck

GEG, Daten und Cybersecurity als Treiber der Zukunft

## 9 Im Gebäudebetrieb entsteht doppelter Handlungsdruck



Im Gebäudebetrieb entsteht ein doppelter Handlungsdruck.

Der Markt erzeugt unmittelbaren Kostendruck durch steigende Energiepreise, CO<sub>2</sub>-Bepreisung und Netzentgelte. Insbesondere bis 2030 ist von einem deutlichen Anstieg dieses Marktdrucks auszugehen. Steigende Energiekosten können dazu führen, dass der Betrieb bestimmter Technologien wirtschaftlich nicht mehr tragfähig ist. Der daraus entstehende Handlungsdruck wirkt unmittelbar.

Gleichzeitig setzt die Regulierung langfristige Ziele und Mindestanforderungen, insbesondere durch EPBD und GEG. Ihre Umsetzung ist im nationalen politisch geprägt. Sie definiert damit den Rahmen für die energetische Entwicklung des Gebäudebestands.

Gleichzeitig stehen unterstützende Instrumente zur Verfügung, insbesondere die Bundesförderung für effiziente Gebäude (BEEG). Sie kann Investitionen in energetische Maßnahmen unterstützen, ändert jedoch nicht den grundlegenden wirtschaftlichen und regulatorischen Handlungsdruck.

Für Betreiber bedeutet dies eine Doppelbelastung: kurzfristiger wirtschaftlicher Druck bei gleichzeitig notwendigen Investitionen in die langfristige Zielerreichung.

Die Regulierung schafft dabei Planungssicherheit und stellt sicher, dass Investitionen langfristig wirksam und geschützt sind.

## 10 Datenbasierter Gebäudebetrieb



Aufbauend auf den zuvor genannten Anforderungen zeigt sich: Performance im Gebäudebetrieb entsteht nicht im Betrieb allein, sondern wird bereits in der Planung angelegt.

Daten, Kennzahlen sowie das Zusammenwirken der Systeme und ihr Verhalten im Betrieb müssen von Beginn an berücksichtigt werden.

Diese Planung wird über ein strukturiertes Inbetriebnahmemanagement in den realen Betrieb überführt.

Erst auf dieser Grundlage können Monitoring und Kennzahlen im Betrieb wirksam genutzt werden.

Darauf aufbauend erfolgt eine kontinuierliche Analyse und Optimierung des Betriebs. Abweichungen werden erkannt und gezielt behoben.

Damit entsteht eine durchgängige Kette von der Planung über die Inbetriebnahme bis hin zum datenbasierten Betrieb.

Diese Kette bildet die Grundlage für einen performanten und nachweisbaren Gebäudebetrieb.



## 11 Praxisbeispiel Gebäudebetrieb



Auf dieser strukturierten Vorgehensweise basiert ein performanter Gebäudebetrieb. Die Realität zeigt jedoch teilweise ein anderes Bild.

Im realen Betrieb treten systematische Abweichungen auf. Anlagen arbeiten nicht wie geplant.

Diese Abweichungen sind kein Einzelfall, sondern treten wiederholt und über viele Gebäude hinweg auf. Ein Beispiel aus der Gebäudewirtschaft der Stadt Köln zeigt, dass in allen untersuchten Liegenschaften Abweichungen festgestellt wurden und ein durchschnittliches Optimierungspotenzial von etwa 10 bis 20 % besteht.

Dieses Potenzial entsteht nicht durch neue Technik, sondern durch die Korrektur des bestehenden Betriebs. Hier greifen Monitoring, Kennzahlen und kontinuierliche Optimierung. Sie machen Abweichungen sichtbar und ermöglichen deren gezielte Behebung.

## 11.1 Beispiel Volumenstromregelung



Ein konkretes Beispiel ist die Volumenstromregelung.

In vielen Anlagen wird der Ventilator auf einen hohen Druck ausgelegt, um alle Betriebszustände sicher abzudecken. Die Volumenstromregler drosseln anschließend lokal auf den tatsächlich benötigten Luftvolumenstrom.

Dadurch wird die Anlage mit einem zu hohen statischen Druck betrieben. Um diesen Druck bereitzustellen, läuft der Ventilator mit unnötig hoher Drehzahl und damit mit erhöhtem Energiebedarf.

Volumenstromregler wie die VRE1/VKE1 sowie VRE1-N/VKE1-N der Wildeboer Bauteile GmbH stellen seit etwa 15 Jahren ein Effizienzsignal zur Verfügung.

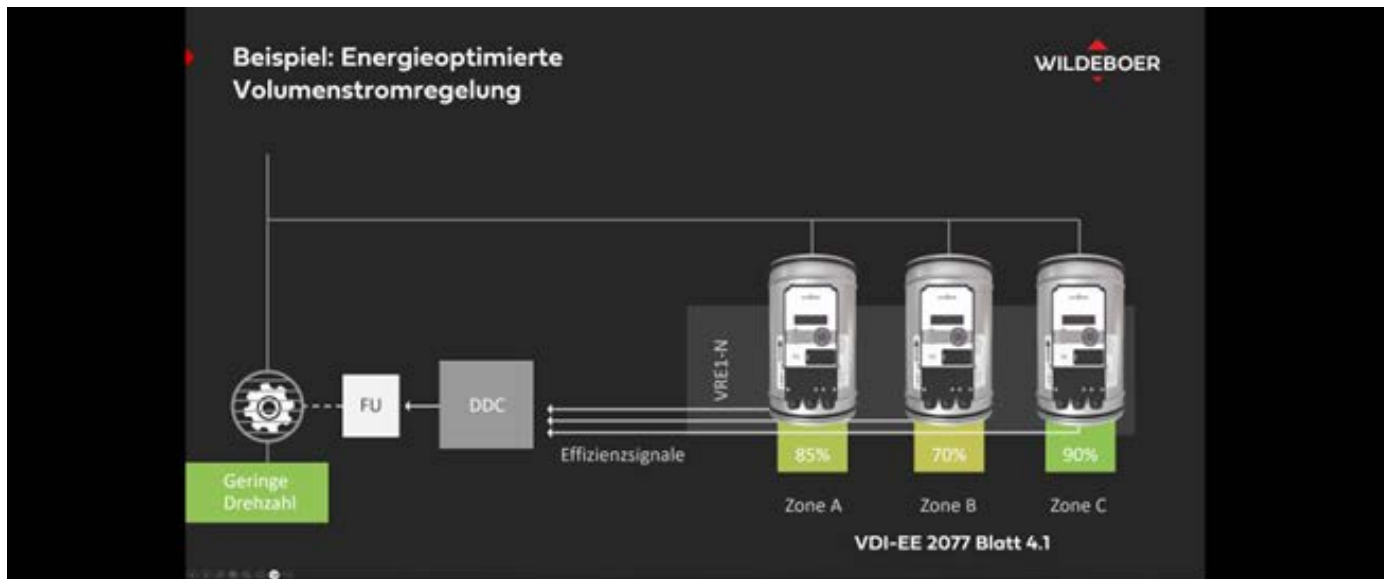
Wird dieses Signal ausgewertet, kann der erforderliche Druck und damit die Ventilatorleistung gezielt reduziert werden, bis der ungünstigste Strang gerade noch ausreichend versorgt wird. Der Betriebspunkt der Anlage verschiebt sich damit in einen deutlich effizienteren Bereich.

In der Praxis wird dieses Signal jedoch häufig nicht genutzt. Die Regelung bleibt statisch, obwohl die notwendigen Informationen vorhanden sind.

Das Ergebnis: vermeidbare Energieverbräuche im laufenden Betrieb.

# Praxisbeispiel Gebäudebetrieb

GEG, Daten und Cybersecurity als Treiber der Zukunft



Neben der Optimierung des Anlagenbetriebs gewinnt die verursachungsgerechte Erfassung von Energieverbräuchen auf Basis realer Betriebsdaten zunehmend an Bedeutung.

In vielen Gebäuden erfolgt die Bewertung weiterhin über Flächenschlüssel. Diese basieren auf statischen Annahmen und berücksichtigen weder das tatsächliche Nutzerverhalten noch den realen Anlagenbetrieb.

Die volumenstrombasierte Erfassung ermöglicht dagegen eine direkte Zuordnung des Energieeinsatzes zu einzelnen Zonen oder Nutzungsbereichen. Grundlage ist der physikalische Zusammenhang zwischen Luftvolumenstrom und Energieeinsatz. Durch die kontinuierliche Erfassung der Volumenströme kann der Energieeinsatz verursachungsgerecht zugeordnet werden.

Die VDI-EE 2077 Blatt 4.1 beschreibt entsprechende Verfahren zur Bewertung von Energieverbräuchen im Gebäudebetrieb.

Für den Flächenschlüsseln ergeben sich folgende Nachteile:

- statische Verteilung ohne Bezug zum Betrieb
- keine Abbildung des Nutzungsverhaltens
- keine Grundlage für eine gezielte Optimierung

Die volumenstrombasierte Erfassung ermöglicht dagegen eine dynamische Zuordnung und schafft die Grundlage für Analyse, Nachweis und Optimierung auf Zonenebene. Sie erweitert das Technische Monitoring um eine verursachungsgerechte energetische Bewertung.

## 12 Rahmenbedingung Cybersecurity



Früher waren IT- und OT-Systeme im Gebäudebetrieb weitgehend getrennt. Anlagen liefen isoliert, häufig mit einem Air-Gap, also ohne direkte Verbindung zu IT-Systemen oder Netzwerken.

Mit der zunehmenden Digitalisierung hat sich das grundlegend verändert. Systeme werden vernetzt, kommunizieren miteinander und sind in IT-Infrastrukturen sowie cloudbasierte Anwendungen eingebunden.

Diese IT/OT-Konvergenz schafft neue Möglichkeiten für Transparenz, Analyse und Optimierung.

Gleichzeitig entstehen neue Abhängigkeiten und Schnittstellen zwischen zuvor getrennten Systemen. Damit steigt die Komplexität im Gebäudebetrieb.

Mit dieser Komplexität entstehen zusätzliche Angriffsflächen.

Cybersecurity wird damit zur grundlegenden Voraussetzung für einen sicheren und stabilen Gebäudebetrieb.

## 12.1 OT wird zum Angriffsziel



OT-Systeme werden zunehmend zum Angriffsziel.

Ursache sind zusätzliche Schnittstellen und externe Anbindungen, etwa durch Fernwartung, Cloud-Integration, mobile Endgeräte oder Übergänge zwischen IT und OT.

Hinzu kommen strukturelle Schwächen im Bestand. Viele Systeme wurden zu einer Zeit entwickelt, in der Cybersecurity keine zentrale Rolle spielte. Lange Lebenszyklen und eingesetzte, teils abgekündigte Betriebssysteme und mangelnde Updatefähigkeit führen dazu, dass bekannte Schwachstellen im Betrieb verbleiben.

Diese Entwicklung wird durch aktuelle Lageberichte bestätigt. Der ENISA Threat Landscape sowie der Lagebericht des Bundesamt für Sicherheit in der Informationstechnik zeigen eine zunehmende Bedrohungslage und eine steigende Anzahl neu entdeckter Schwachstellen, auch im OT-Umfeld.

## 12.2 Cybersecurity ist systemisch geregelt



Cybersecurity muss heute ganzheitlich betrachtet werden.

Auf Produktebene greifen regulatorische Anforderungen wie der Cyber Resilience Act, ergänzt durch Regelwerke wie RED und GPSR.

Im Betrieb werden diese Anforderungen durch die NIS2-Richtlinie adressiert. Sie definiert organisatorische und technische Maßnahmen für den sicheren Betrieb. Die zugrunde liegenden Konzepte sind nicht auf KRITIS beschränkt, sondern grundsätzlich auf alle Gebäude übertragbar.

Zwischen diesen Ebenen stehen Normen. Standards wie ISO 27001 und insbesondere die IEC 62443 übersetzen regulatorische Anforderungen in konkrete technische und organisatorische Maßnahmen.

Erst im Zusammenspiel von Produkthanforderungen, Betriebsanforderungen und normativer Umsetzung entsteht eine mehrschichtige Sicherheitsarchitektur.

Cybersecurity ist damit kein Einzelaspekt, sondern das Ergebnis einer ganzheitlichen Strategie.

## 12.3 Sichere Produkte sind Voraussetzung



Mit dem Cyber Resilience Act werden Anforderungen an die Sicherheit von Produkten über den gesamten Lebenszyklus definiert.

Ausgangspunkt ist Security-by-Design. Sicherheitsanforderungen werden bereits in der Entwicklung berücksichtigt. Dazu gehören Bedrohungsanalysen, die Identifikation von Angriffsflächen sowie die Umsetzung sicherer Kommunikations- und Zugriffskonzepte. Auch die Auswahl eingesetzter Softwarekomponenten erfolgt unter Sicherheitsgesichtspunkten.

Darauf aufbauend folgt Security-by-Default. Produkte müssen im Auslieferungszustand sicher konfiguriert sein. Dazu gehört auch, dass sie ohne bekannte Schwachstellen ausgeliefert werden und jederzeit auf eine sichere Grundeinstellung zurückgesetzt werden können.

Ein zentraler Bestandteil ist das Schwachstellenmanagement. Sicherheitslücken müssen kontinuierlich identifiziert, bewertet und behandelt werden. Dazu gehört auch die systematische Prüfung der Produkte gegen Schwachstellendatenbanken.

Die Grundlage dafür ist Transparenz über die eingesetzten Komponenten, über eine Software Bill-of-Materials. Damit wird auch die Lieferkette in die Sicherheitsbetrachtung einbezogen.

Ergänzt wird dies durch klare Prozesse für den Umgang mit Schwachstellen, etwa über eine Coordinated Vulnerability Disclosure Policy (CVD-Policy) sowie die Veröffentlichung von Security Advisories.

Ebenso erforderlich sind Sicherheitsinformationen für den Betrieb. Hersteller müssen dokumentieren, wie Produkte über den gesamten Lebenszyklus cybersicher verwendet werden können, einschließlich verbleibender Restrisiken sowie empfohlener Schutzmaßnahmen.

Dafür ist die Updatefähigkeit entscheidend. Produkte müssen über ihren gesamten Lebenszyklus hinweg sicher aktualisierbar sein.

Diese Anforderungen greifen ineinander und begleiten das Produkt über seinen gesamten Lebenszyklus.



## 12.4 Achtung bei Produkten ohne Updatefähigkeit



In der Praxis werden Gebäudeautomationssysteme über lange Zeiträume geplant und umgesetzt. Dabei kommen häufig auch Komponenten zum Einsatz, die bereits vor Inkrafttreten der CRA-Anforderungen in Verkehr gebracht wurden.

Problematisch wird es dann, wenn diese Komponenten nicht mehr dem aktuellen Stand der Sicherheit entsprechen, etwa weil keine Updates oder kein sicherheitsrelevanter Support mehr verfügbar sind.

Entscheidend ist jedoch die regulatorische Entwicklung:

Ab Dezember 2027 müssen neu in Verkehr gebrachte Produkte mit digitalen Elementen die Anforderungen des CRA erfüllen.

Das bedeutet: Auch Komponenten die vor Dezember 2027 in Verkehr gebracht wurden, werden relevant, sobald sie Teil eines neuen Systems werden.

Sobald diese Komponenten im Rahmen eines neuen Systems integriert und als Teil eines neuen Produkts in Verkehr gebracht werden, greifen die Anforderungen grundsätzlich auf das Gesamtsystem.

Maßgeblich ist dabei nicht das ursprüngliche Inverkehrbringen der Einzelkomponenten, sondern das Inverkehrbringen des Gesamtsystems.

Damit entsteht ein klares Risiko: Ein System kann zukünftig nicht CRA-konform sein, obwohl einzelne Komponenten heute noch zulässig sind.

Cybersecurity ist damit keine isolierte Produkteigenschaft, sondern eine Anforderung an das Gesamtsystem. Integration macht aus Altkomponenten ein neues CRA-relevantes Produkt.

## 12.5 Sicherheit entsteht im Betrieb



Im Gebäudebetrieb entsteht Sicherheit nicht durch einzelne Maßnahmen, sondern durch ein strukturiertes Vorgehen im Betrieb.

Diese Anforderungen entsprechen den grundlegenden Prinzipien der NIS2-Richtlinie. Sie gelten unabhängig von der Einstufung als kritische Infrastruktur als Grundlage für den sicheren Betrieb vernetzter Systeme.

Ausgangspunkt ist ein durchgängiges Risikomanagement und ein darauf aufbauendes Sicherheitskonzept. Risiken müssen systematisch identifiziert, bewertet und behandelt werden.

Darauf aufbauend folgt die Zugriffskontrolle und das Identitätsmanagement. Nur berechtigte Personen dürfen Zugriff auf Systeme, Funktionen und definierte Bereiche erhalten.

Ein zentraler Bestandteil ist das Incident Management. Sicherheitsvorfälle müssen erkannt, bewertet und strukturiert behandelt werden.

Ebenso wichtig ist die Sicherstellung der Betriebsfähigkeit. Business Continuity und Wiederanlaufkonzepte stellen sicher, dass Systeme auch im Störfall verfügbar bleiben.

Ergänzt wird dies durch klare Governance-Strukturen, Schulungen und definierte Verantwortlichkeiten. Sicherheit muss organisatorisch verankert sein.

Diese Elemente greifen ineinander und wirken kontinuierlich im Betrieb.

Cybersecurity wird im Gebäudebetrieb durch kontinuierliches Risikomanagement maßgeblich unterstützt.



## 12.6 Schwachstellenmanagement im Gebäudebetrieb



Cybersecurity im Gebäudebetrieb entsteht im Zusammenspiel von Hersteller und Betreiber.

Auf Herstellerseite werden Schwachstellen systematisch identifiziert, bewertet und über definierte Prozesse behandelt. Grundlage sind unter anderem SBOMs, Schwachstellendatenbanken und interne PSIRT-Strukturen. Im Rahmen eines Coordinated Vulnerability Disclosure Prozesses werden relevante Informationen gebündelt und in Form von Security Advisories bereitgestellt.

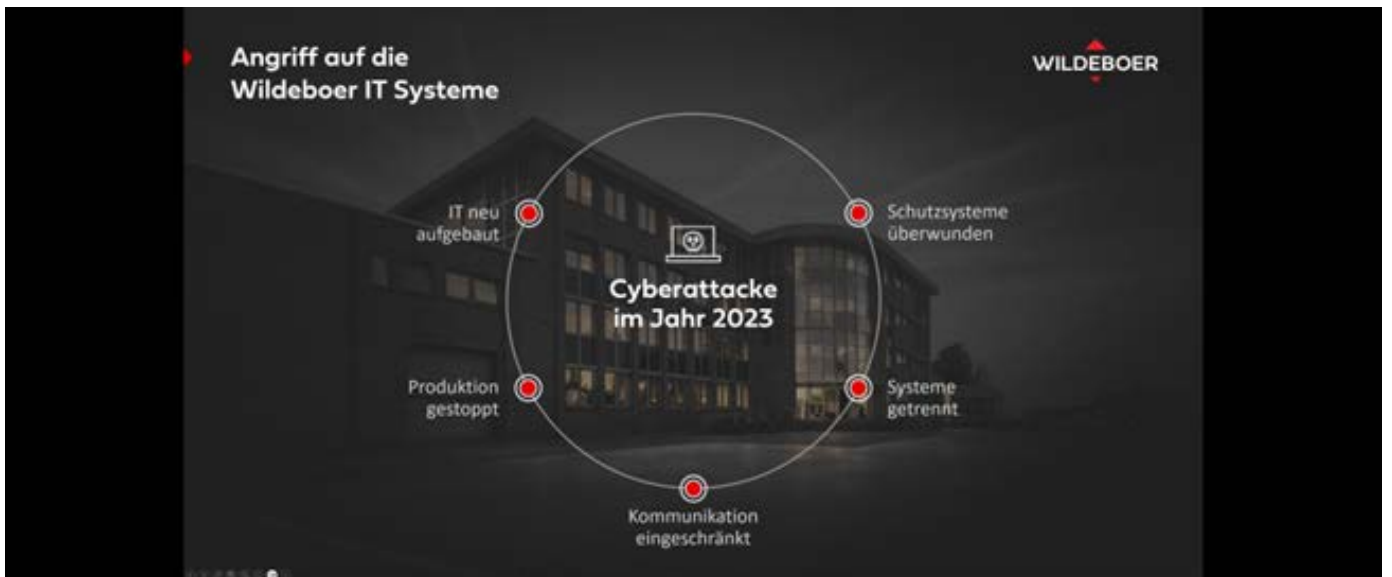
Diese Advisories beschreiben, welche Maßnahmen erforderlich sind. Ergänzend stellen Produktsicherheitsinformationen dar, wie diese Maßnahmen im konkreten System umzusetzen sind.

Auf Betreiberseite erfolgt die Zuordnung dieser Informationen zu den eingesetzten Assets. Voraussetzung ist eine aktuelle Asset-Datenbasis. Durch den kontinuierlichen Abgleich von Assets mit veröffentlichten Advisories werden betroffene Systeme identifiziert.

Darauf aufbauend erfolgt die Risikobewertung, Priorisierung und Umsetzung der erforderlichen Maßnahmen im Betrieb.

Cybersecurity entsteht damit nicht isoliert, sondern durch einen kontinuierlichen Informations- und Umsetzungsprozess zwischen Hersteller und Betreiber.

## 12.7 Praxisbeispiel Cyberangriff



Das ist kein theoretisches Szenario.

Ein Cyberangriff betrifft nicht nur IT-Systeme, sondern die gesamte Organisation. Systeme müssen getrennt werden, um eine Ausbreitung zu verhindern. Die Kommunikation zu Kunden und Partnern ist eingeschränkt oder fällt aus.

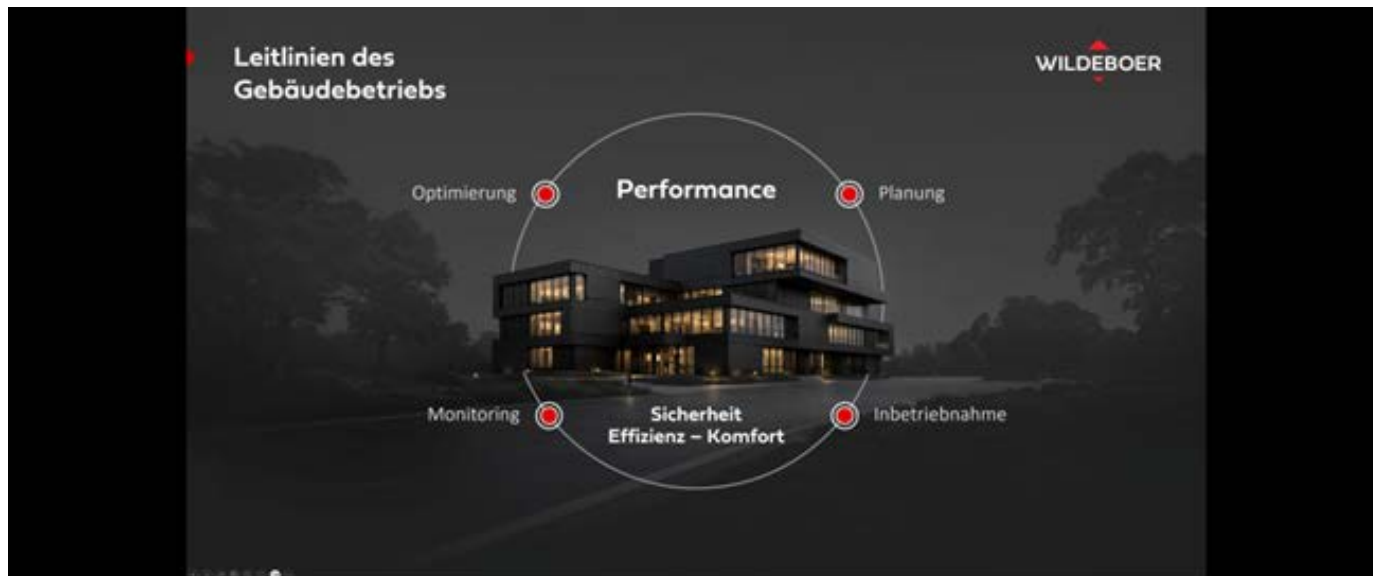
Gleichzeitig kommt die Produktion zum Stillstand. Produkte können nicht mehr hergestellt und ausgeliefert werden.

Parallel dazu müssen Ersatzprozesse aufgebaut und Infrastrukturen neu hergestellt werden. Das hat unmittelbare wirtschaftliche Auswirkungen, sowohl für das Unternehmen als auch für die Kunden.

Genau in solchen Situationen zeigt sich, ob Systeme beherrschbar sind und ob die notwendigen Strukturen und Fähigkeiten vorhanden sind.



## 13 Leitlinien des Gebäudebetriebs



Die Performance im Gebäudebetrieb entsteht nicht durch Einzelmaßnahmen, sondern durch ein abgestimmtes Vorgehen über den gesamten Lebenszyklus.

Ausgangspunkt ist die Planung. Hier wird die Systemarchitektur, die Datenstruktur und die Kennzahlen zur Bewertung festgelegt.

Darauf aufbauend folgt die Inbetriebnahme. Sie stellt sicher, dass die geplanten Funktionen, die Einstellung und das Zusammenspiel der Systeme im realen Betrieb tatsächlich umgesetzt sind.

Im Betrieb selbst zeigt sich dann die erreichte Performance auf der Basis der Kennzahlen. Hier wirken die Systeme unter tatsächlichen Nutzungs- und Randbedingungen zusammen.

Die Grundlage für die Bewertung bildet das Monitoring. Es schafft Transparenz über Energieverbräuche, Zustände und Abweichungen.

Auf dieser Basis erfolgt die kontinuierliche Optimierung. Betriebsstrategien werden angepasst und Systeme werden gezielt verbessert.

Diese Schritte greifen ineinander und bilden einen geschlossenen Regelkreis.

Erst dieses Zusammenspiel ermöglicht eine dauerhaft nachweisbare Performance im Gebäudebetrieb.

## 14 Produktinweis



Für einen sicheren und performanten Gebäudebetrieb ist die koordinierte Ansteuerung brandschutztechnischer Komponenten entscheidend.

Mit WiNet stellen wir eine durchgängige Systemlösung zur Verfügung, die Brandschutzklappen und Rauchauslöseeinrichtungen strukturiert vernetzt und steuerungstechnisch zusammenführt.

Auslösegruppen können systemübergreifende ohne Programmierung parametrisiert und logisch verknüpft werden, sodass auch komplexe Abschottungsszenarien sicher umgesetzt werden.

Automatische Adressierung und unterstützte Inbetriebnahme reduzieren den Aufwand und erhöhen die Umsetzungsqualität.

Damit entsteht die Grundlage für:

- eine sichere Funktion im Brandfall,
- eine beherrschbare Systemstruktur,
- Planungssicherheit,
- einen effizienten Betrieb sowie eine einfache Funktionsprüfung der Brandschutzklappen.

Rauchauslöseeinrichtungen übernehmen die frühzeitige Detektion von Rauch in Lüftungsleitungen und lösen definierte Schutzmaßnahmen aus.

Sie steuern gezielt Brandschutzklappen, Rauchschutzklappen und Ventilatoren an oder binden Signale in die Gebäudeleittechnik ein.

Dadurch werden Abschottungsszenarien automatisch aktiviert und eine Rauchübertragung zwischen Brandabschnitten verhindert.

Alarm- und Störungsspeicherung sowie normgerechte Zulassungen (VdS, DIBt) stellen die zuverlässige Funktion sicher.

Damit leisten Rauchauslöseeinrichtungen einen zentralen Beitrag zur Betriebsicherheit.

## 15 Whitepaper



Safety wurde im Rahmen dieses Vortrags nicht im Detail behandelt.

Ein ergänzendes Whitepaper adressiert die Betriebsicherheit in RLT-Anlagen und betrachtet systemische Sicherheitsanforderungen in der Luftverteilung.

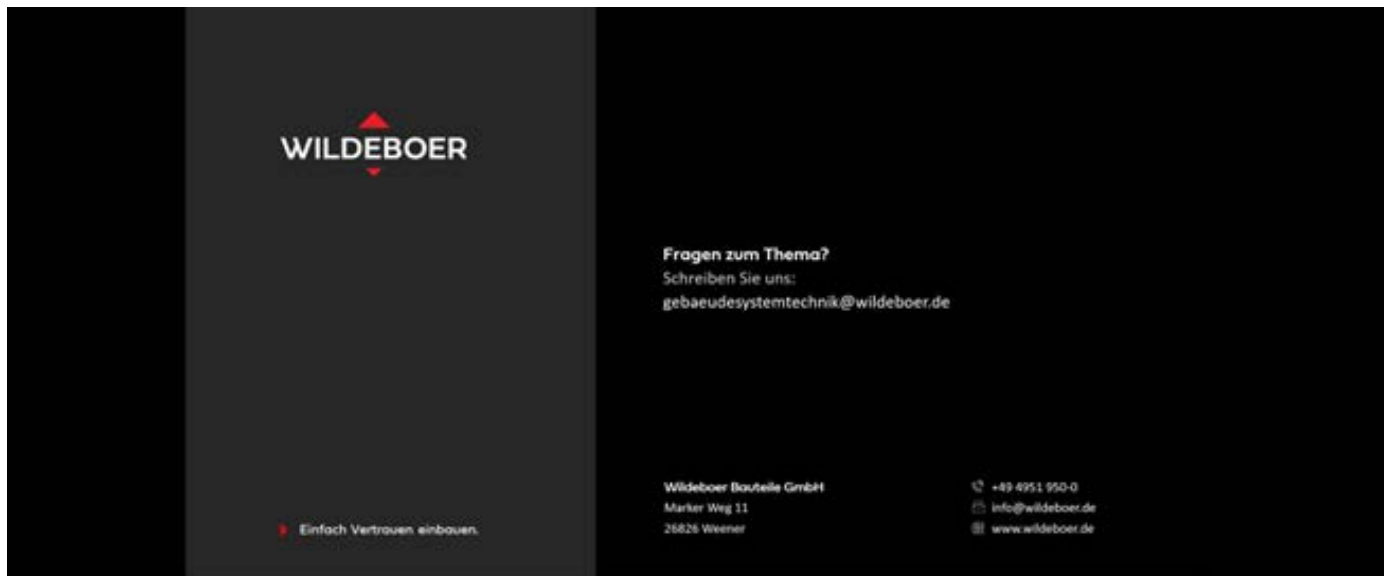
### 15.1 Whitepaper zum Vortrag



Der Vortrag wird durch ein begleitendes Whitepaper ergänzt.

Es enthält weiterführende Informationen, Einordnungen und vertieft die dargestellten Zusammenhänge über den gesamten Lebenszyklus des Gebäudebetriebs.

## 16 Abschluss



Wir freuen uns über den fachlichen Austausch mit Ihnen.

Schreiben Sie uns gerne: [gebaeudesystemtechnik@wildeboer.de](mailto:gebaeudesystemtechnik@wildeboer.de)





# Immer für Sie da

Standorte & Kontakt

**WILDEBOER**

Werk - Verwaltung  
+49 4951 950-0  
info@wildeboer.de  
www.wildeboer.de

Utrecht

**WILDEBOER**

Büro Utrecht  
+31 30 767 0150  
info@utrecht.wildeboer.eu  
www.wildeboer.de/nl

Leipzig

**WILDEBOER**

Niederlassung Leipzig  
+49 34444 310-0  
info@leipzig.wildeboer.de  
www.wildeboer.de

Ulm

**WILDEBOER**

Niederlassung Ulm  
+49 7392 9692-0  
info@ulm.wildeboer.de  
www.wildeboer.de

Other locations marked on the map: Weener, Hamburg, Hannover, Berlin, Köln, Frankfurt, Stuttgart, München.

