

KNX

BACnet

MQTT

Modbus

OPC  
(DA/UA)

SNMP

Fidelio/Opera | Protel | Infor  
RMS Cloud | CharPMS  
VingCard Web | Kaba | Salto

DALI EnOcean  
M-Bus DMX

Proprietäre Lösungen

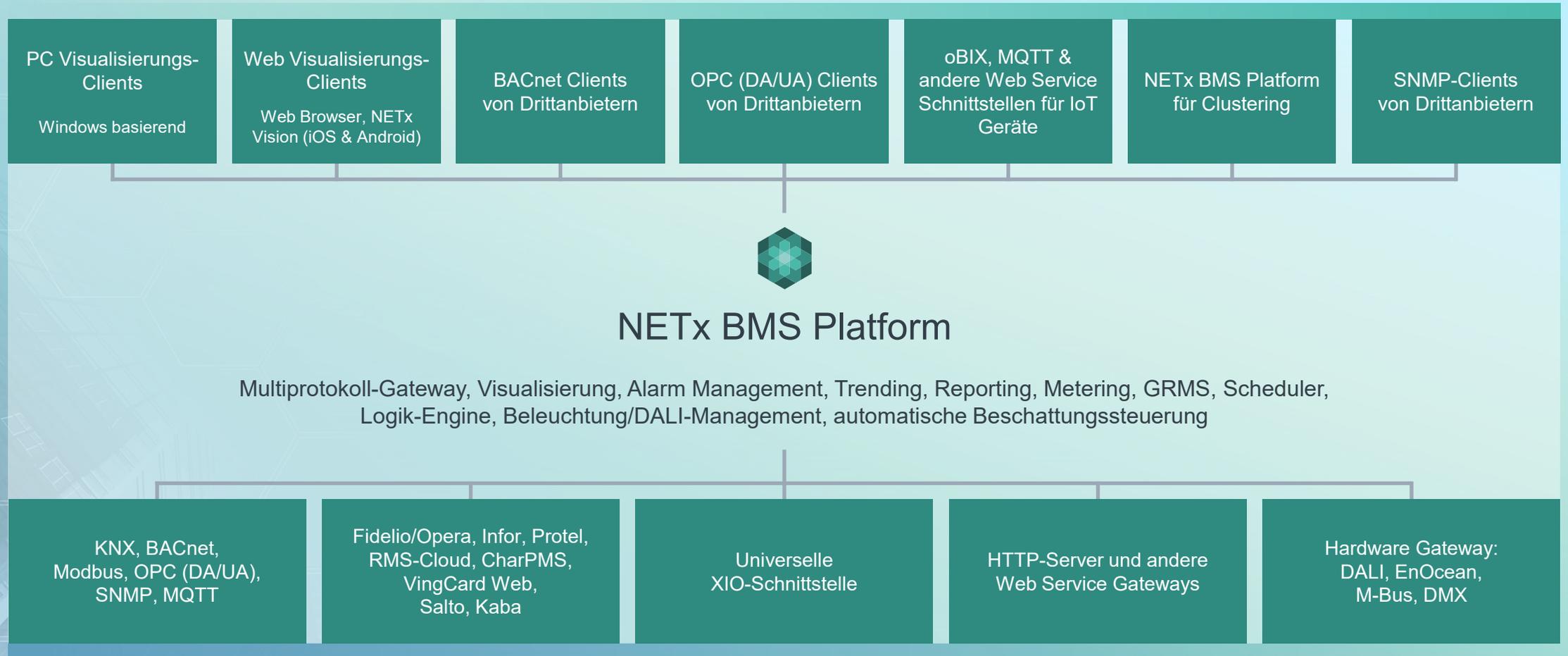
# All-in-one

**Gebäudeautomatisierungssoftware für  
mittlere und große Projekte der  
Gebäudeautomation**

Gebäudemanagementsysteme für die Bereitstellung von  
Sicherheit in existierenden KNX-Projekten:

Organisatorische Maßnahmen und Geräteüberwachung

<p>Österreichisches, weltweit tätiges Unternehmen — gegründet 2001</p>	<p><b>20</b> Jahre Erfahrung</p>	<p><b>100+</b> Ländern vertreten</p>	<p>Softwarelösungen für Gebäudeautomationsysteme</p>
<p>Unsere Kunden</p>	<p><b>500.000+</b> Projekte mit 500.000+ Datenpunkten</p>		<p>Integration von heterogenen Gebäudeautomationsnetzwerken: Gebäudemanagementsystem Plattform (BMS Plattform), OPC Server</p>
<ul style="list-style-type: none"><li>• Elektroplaner</li><li>• Elektroinstallateure</li><li>• Systemintegratoren</li></ul>	<p><b>8.000+</b> aktive Lizenzen</p>	<p><b>40</b> internationale Verkaufs- und F&amp;E Partner</p>	<p>Managementapplikationen: Visualisierung, Energiereporting, Automatische Beschattungs- steuerung, Lichtsteuerung, Projektsupport</p>



## Ist Sicherheit in der Haus- und Gebäudeautomation wichtig?

- “Warum sollte es mich stören, wenn jemand mein Licht ein- oder ausschaltet”
- “Wenn jemand meine Raumtemperatur wissen möchte, habe ich keine Einwände”

## Sicherheitskritische Leistungen

- Zugangskontrolle
- Einbruchalarm

## Vandalismusakte können massive, wirtschaftliche Folgen haben

- Komplette Abschaltung des Systems im Hotel
- Sicherheitsangriffe in funktionellen Gebäuden
- Massenpanik in öffentlichen Räumen (z.B. Beleuchtungssystem in Konzerthallen)
- Krankenhäuser (z.B. Beleuchtungssystem in der Notaufnahme)
- Gebäudesystem kann Eintrittspunkt für andere (kritischere) Systeme zB (Hotelmanagementsystem) sein

## Was ist mit Sicherheit in der Gebäudeautomation?

Alle Protokolle (KNX, Modbus, BACnet, proprietäre Lösungen) sind oder waren anfällig für Sicherheitsangriffe

Die gute Nachricht ist, es sind neue Sicherheitsstandards für KNX verfügbar

### KNX Datensicherheit

Sichere Kommunikation für alle KNX-Medien

### KNX IP-Sicherheit

Zusätzliche Sicherheitsmaßnahmen für KNX über IP-Netzwerke

## Ist KNX-Sicherheit genug?

Ja, es verwendet modernste kryptografische Technologien wie sie auch in anderen Anwendungsbereichen verwendet werden (TLS/SSL, e-banking, ...)

Aber:

Was passiert mit existierenden KNX-Projekten, die keine sicheren KNX-Geräte verwenden?

Sichere Kommunikation allein reicht nicht aus

Beispiel:

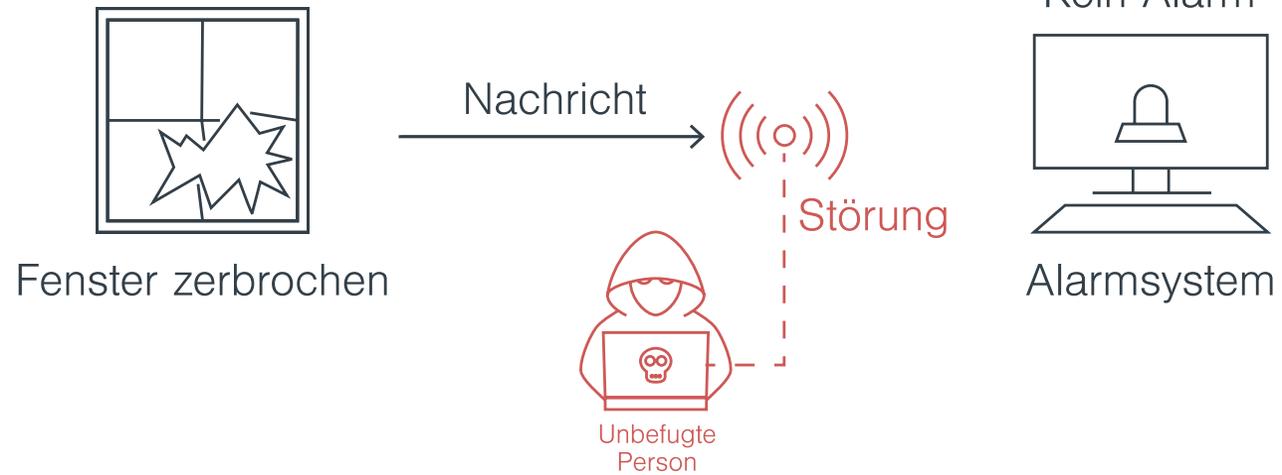
Denial-of-service-Angriff im  
Alarmsystem

Nachricht vom Glasbruchsensor,  
wenn die Fensterscheibe bricht



Jamming-Angriff bricht das Alarmsystem vollständig

Nachricht wird vom Alarmsystem nicht empfangen



## Sicherere Lösung: Sensor sendet regelmäßig "OK" Nachricht



## Fehlt die Nachricht, wird ein Alarm ausgelöst



## Verwendung von organisatorischen Maßnahmen

- Isolation von Gebäudeautomationsnetzwerken
- Verwendung von gestaffelten Methoden (defence in depth)
- Schulung der Elektroinstallateure und Integratoren für die richtige und sichere Anwendung von Technologien

## Verwendung zusätzlicher Software Tools auf der Gebäudemanagementebene

Gebäudemanagementsysteme (BMS) bieten zusätzliche Gegenmaßnahmen gegen Sicherheitsangriffe

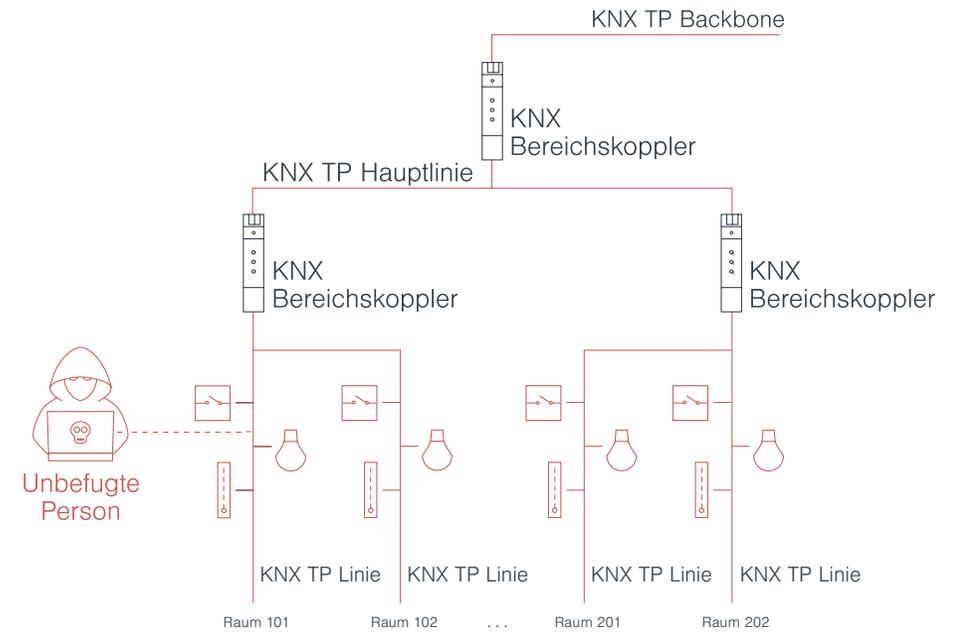
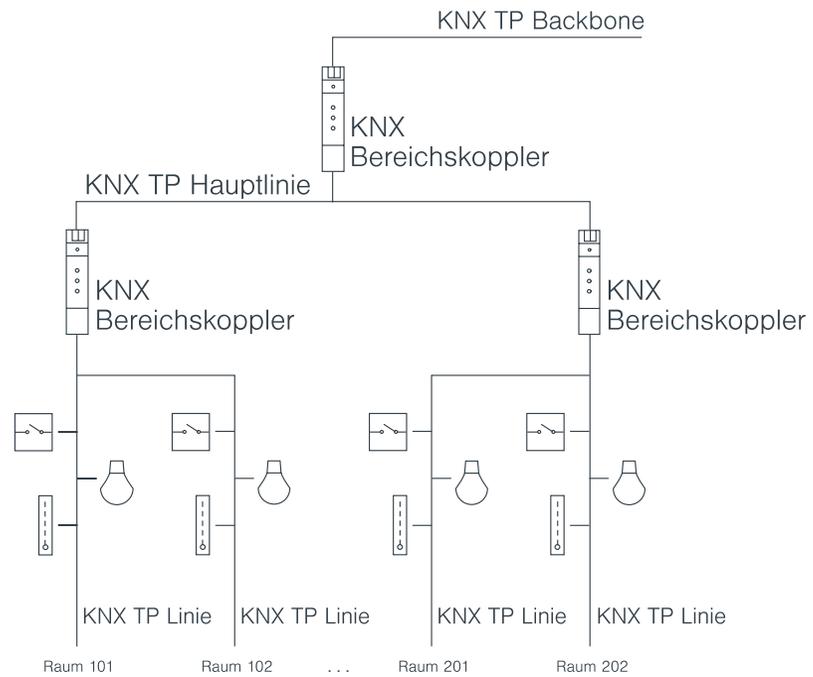
Intrusion Detection

Geräteüberwachung und  
Protokollierung

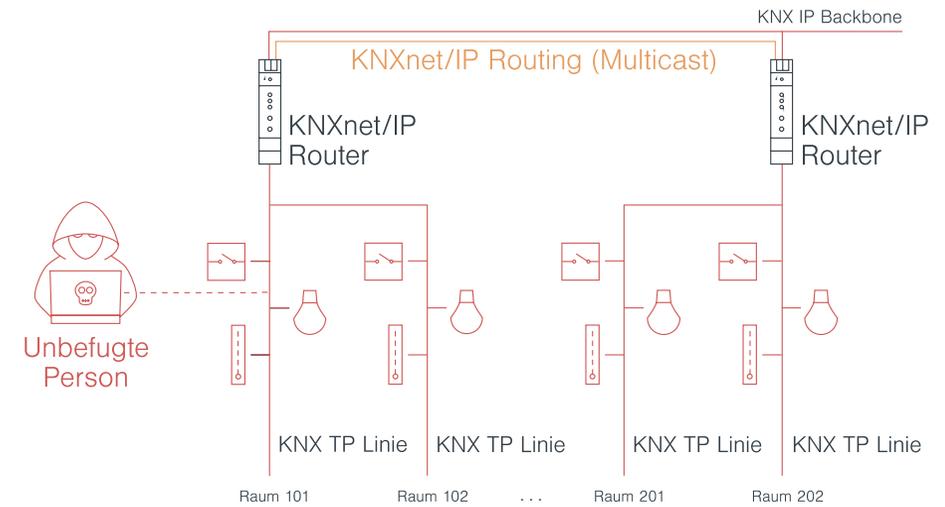
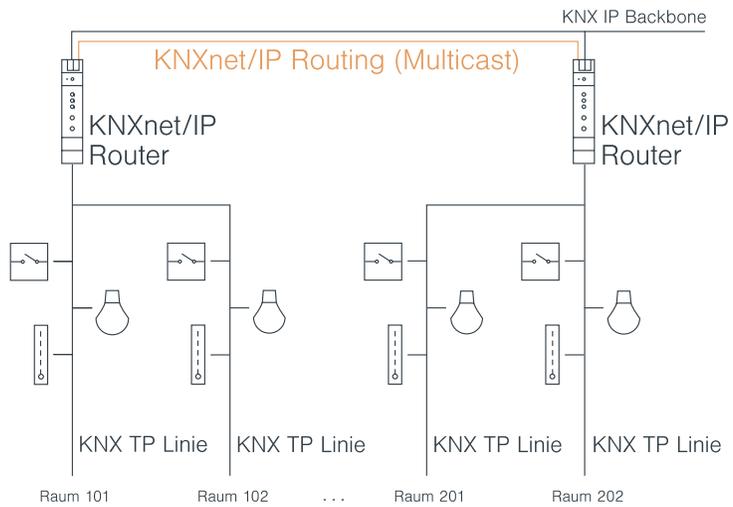
Alarmsysteme

Visualisierungen, die TLS-  
Verbindungen unterstützen

## Unsichere Integration

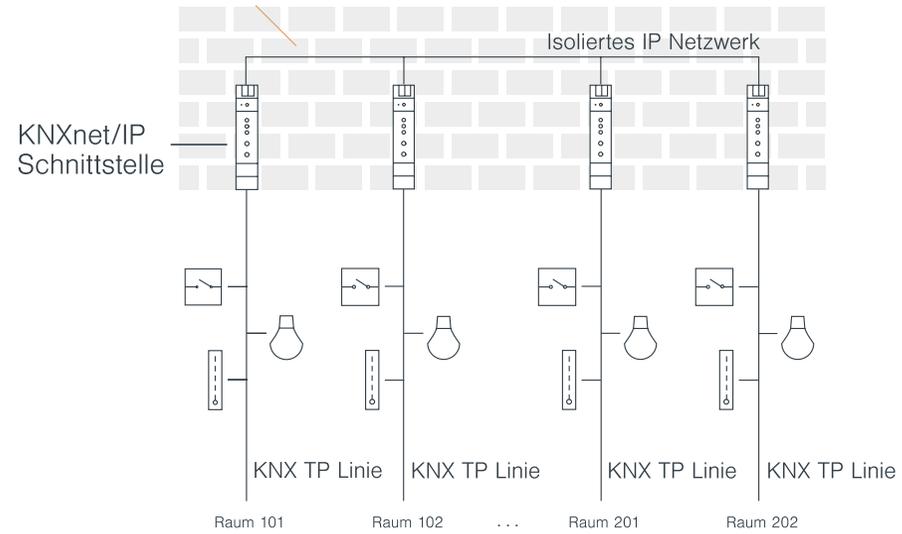


## Besser, aber immer noch unsicher

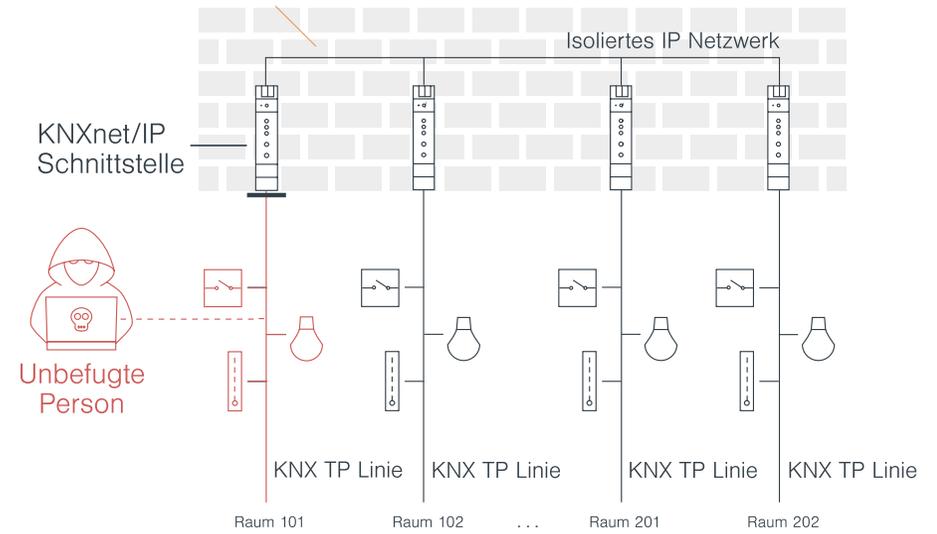


## Sicherheit durch isolierte Räume

Kein KNXnet/IP Routing!



Kein KNXnet/IP Routing!



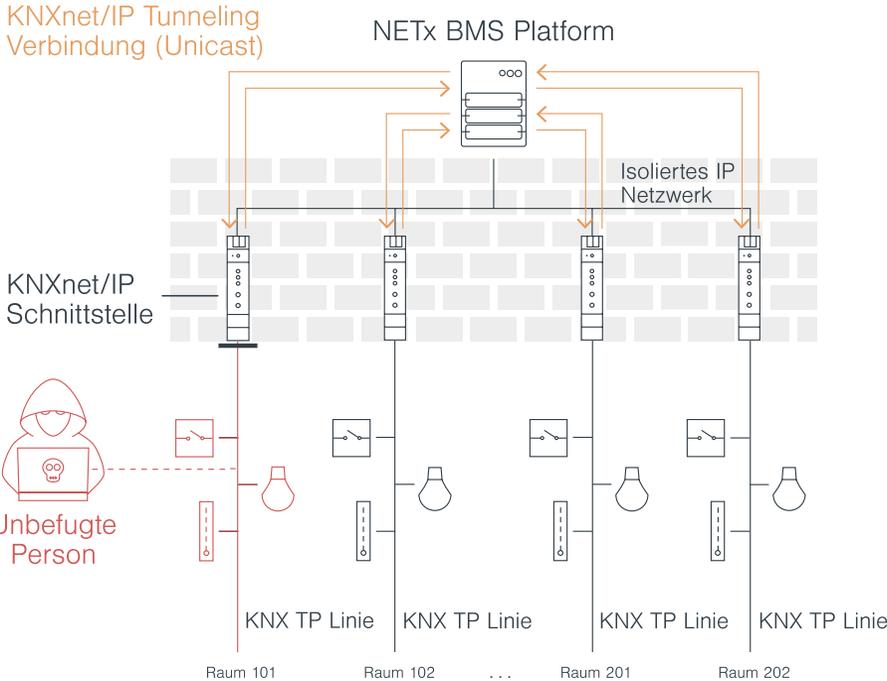
## Zwischen den Räumen ist keine KNX-Kommunikation notwendig

- Kein KNXnet/IP-routing notwendig
- KNXnet/IP-Schnittstellen anstelle von KNXnet/IP-Routern (um einiges billiger)

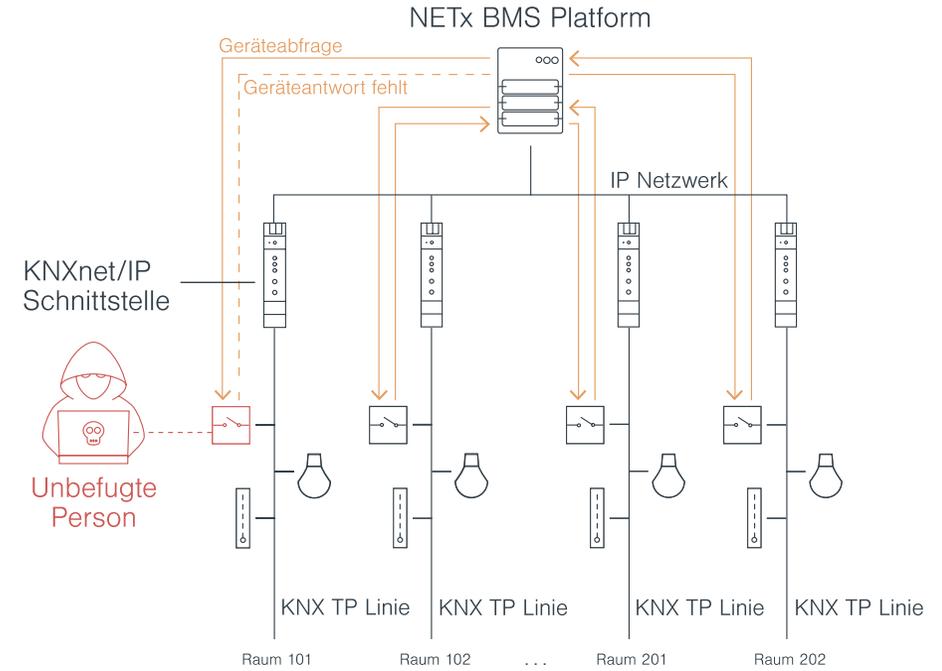
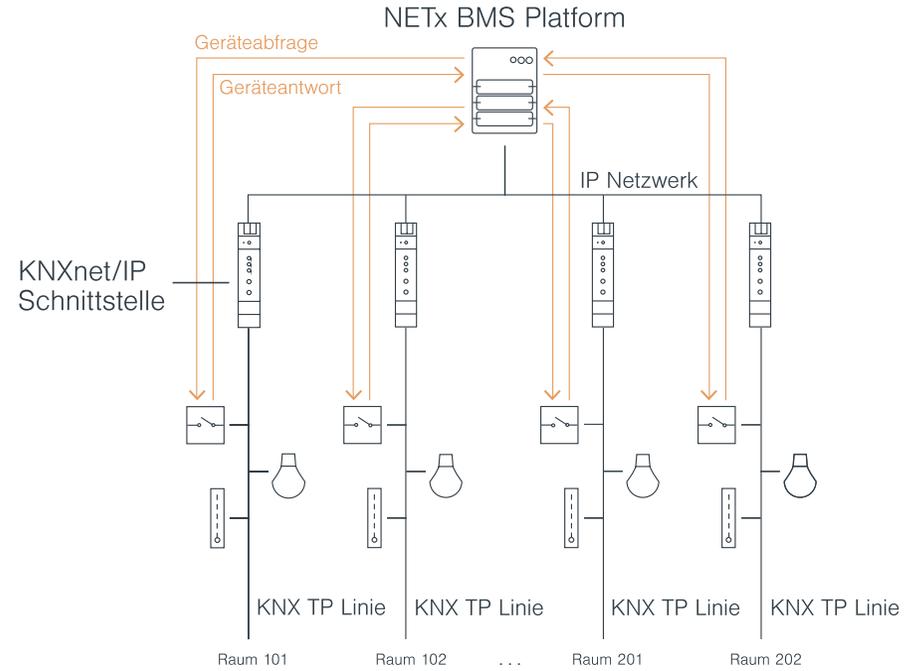
## Was ist mit zentralen Befehlen, wie der Änderung des Sollwerts?

- Einsatz von Gebäudeautomationssoftware (BMS)

## Sicheres, zentrales Management durch verwenden einer BMS-Lösung



## Geräteüberwachung



# Intrusion Detection mit BMS

Geräteabfrage mit KNX Managementanfrage

Antwortet das Gerät nicht innerhalb einer bestimmten Zeit, wird ein Alarm ausgelöst

Kein Bandbreitenproblem durch mehrere Punkt-zu-Punkt Tunnelling-Verbindungen

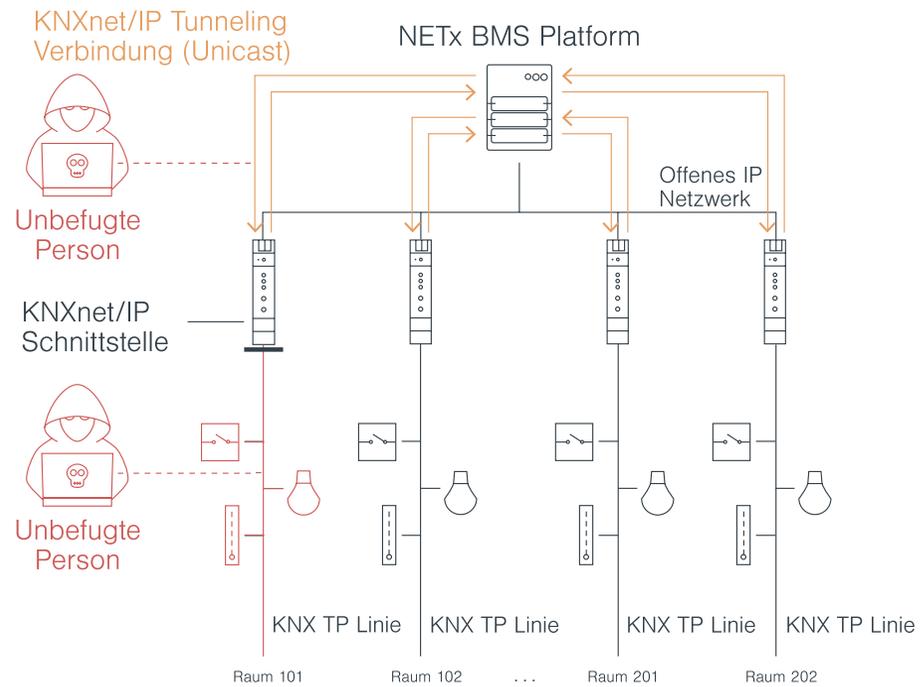
Datenquelleninformationen sind ebenfalls vorhanden

172.16.3.1		
GATEWAY		True
Status	KNX Gateway status number	0
Devices		
05 - Floor1		
0 - Lighting		
000	Room101 Dimming - Switch	True
001	Room101 Dimming - Switch - Status	True
002	Room101 Dimming - Rel Dimming	???
002 - SEND	Trigger to send the KNX telegram	False
002.Control	Room101 Dimming - Rel Dimming / I...	???
002.StepCode	Room101 Dimming - Rel Dimming / ...	???
004	Room101 Dimming - Brightness - Sta...	100

Item timestamp	4	02.02.2017 12:23:07
Item Access Rights	5	READ
Server Scan Rate	6	10
Item Unit	100	
Item Description	101	Room101 Dimming - Switch - Status
High Value Limit	102	
Low Value Limit	103	
Item Local Timestamp	400	02.02.2017 13:25:07
Handle	1000	994
Access Level	1001	0
Persistent	1002	False
Historical	1003	False
Redundant	1004	True
Source	1005	SYS:KNX;SRC:172.16.3.1;ADR:05.03.001

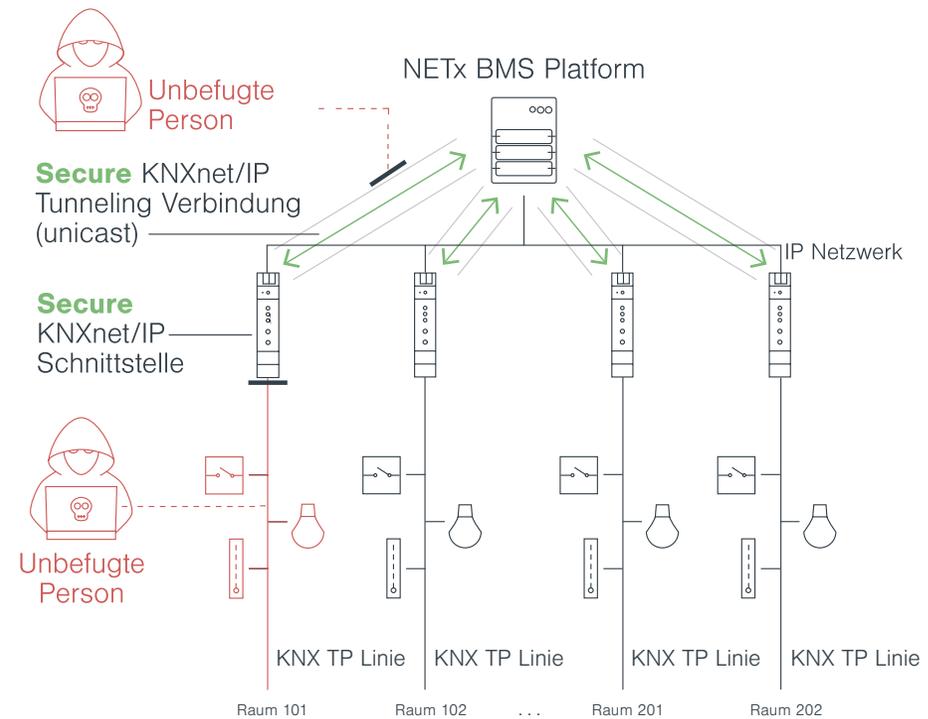
Was tun, wenn das IP-Netzwerk nicht isoliert werden kann?

Verwendung von KNX Security Standard:  
sicheres KNXnet/IP Tunnelling



Neue KNXnet/IP-Security schützt die Kommunikation zwischen der BMS Platform und den KNXnet/IP-Routern und Schnittstellen

Unbefugte Personen mit Zugang zum IP-Netzwerk können die KNXnet/IP-Kommunikation nicht stören



## Sichere Visualisierung mit der NETx BMS Plattform

Die NETx BMS Plattform ermöglicht webbasierte Visualisierung

Nur HTML5 und JavaScript  
https Support unter  
Verwendung von TLS

Benutzername/Passwort  
Authentifizierung



Erhältlich für die  
BMS Platform

Sicheres KNXnet/IP-  
Tunnelling

Kann mit neuen,  
sicheren KNXnet/IP-  
Routern und  
-Schnittstellen  
verwendet werden

[www.netxautomation.com](http://www.netxautomation.com)