Gebäudeautomationssysteme zur Bereitstellung von Security in bestehenden KNX Projekten: Organisationale Maßnahmen und Geräteüberwachung

Teil 2: Bestehende Projekte sicher gestalten

Um gefährliche Sicherheitslücken in bereits bestehenden KNX Projekte zu vermeiden, können unterschiedliche organisatorische Maßnahmen umgesetzt werden:

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

Zusätzliche Software Tools auf der Gebäudemanagementebene können die Sicherheit noch erhöhen z.B.

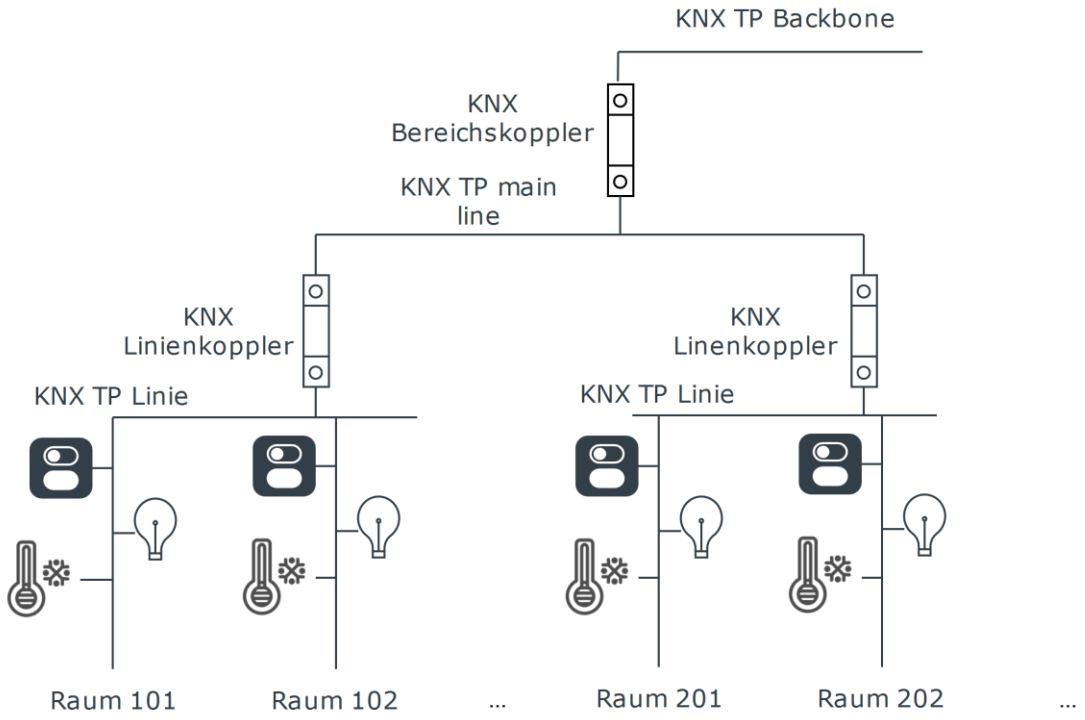
- Intrusion Detection
- Alarmsysteme
- Geräteüberwachung und Protokollierung
- Visualisierungen, die TSL/SSL Verbindungen unterstützen

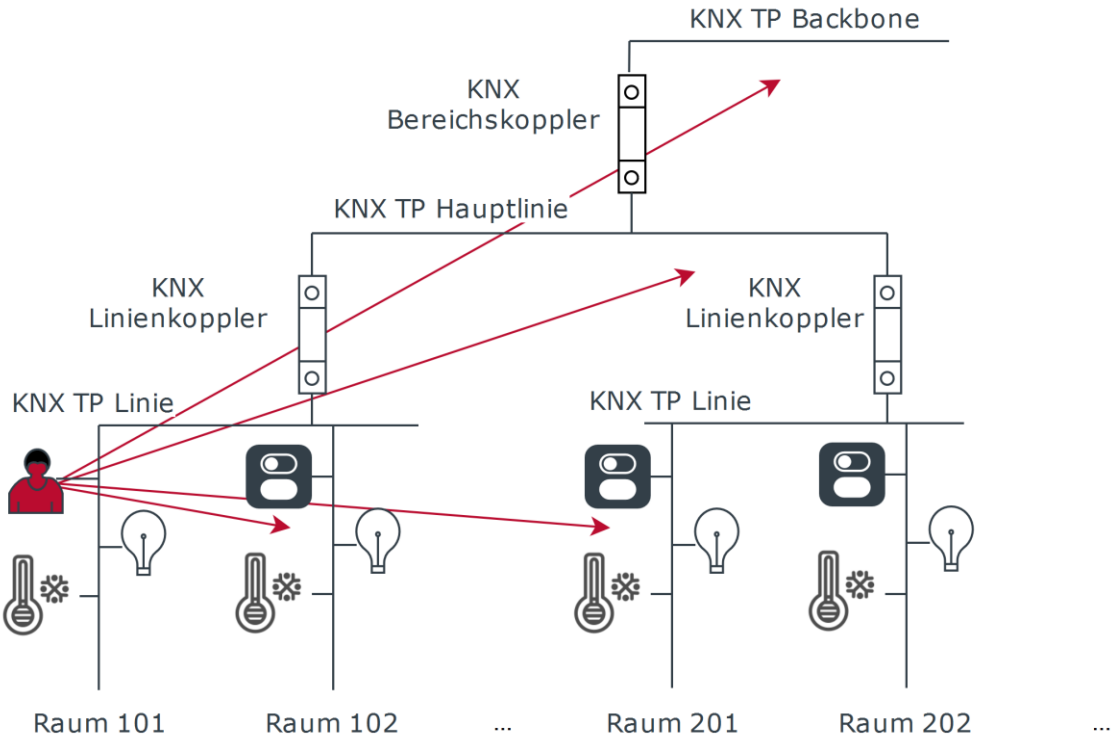
Mit den nachfolgenden Beispielen zeigen wir, wie Sie bestehende Gebäudeautomations-projekte sicherer gestalten:

Defence in Depth in Hotelprojekten

Beispiel 1: Unsichere Integration

Die folgende Grafik zeigt den typischen Aufbau eines Gebäudeautomationssystems unter Verwendung von Bereichs- und Linienkopplern. Ein Angreifer kann sich Zugriff auf das gesamte KNX Netzwerk verschaffen, indem er z.B. ein KNX Gerät entfernt und dadurch Zugang zum entsprechenden BUS-Kabel hat. Linien- und Bereichskoppler filtern zwar grundsätzlich den Datenverkehr allerdings ist das Filtern oft nicht möglich (z.B. zentrale Visualisierung am Backbone) oder deaktiviert.

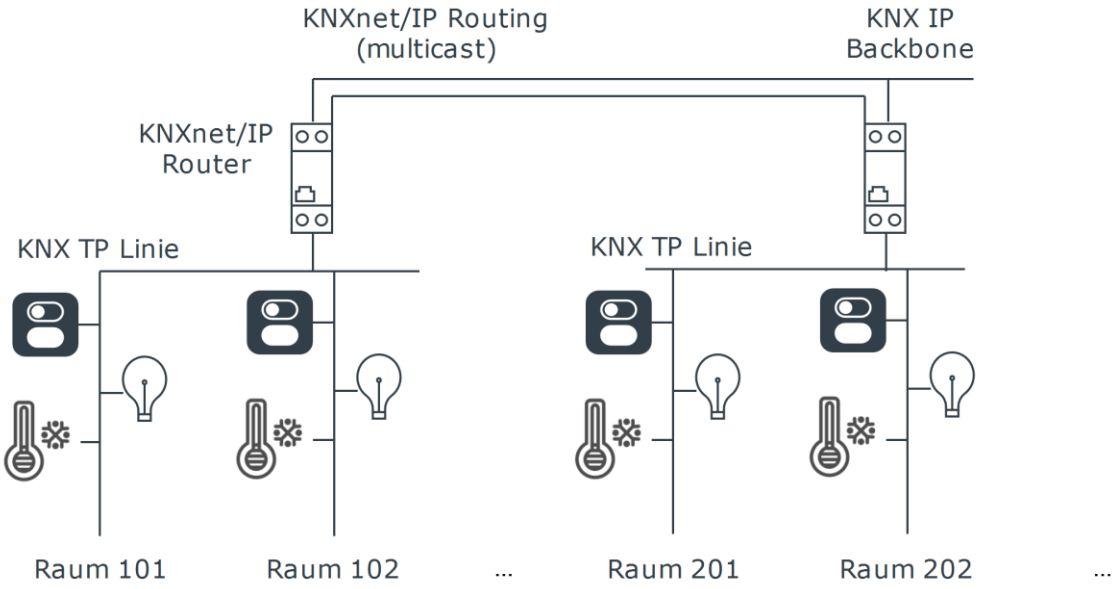

KNX TP Backbone
KNX
Bereichskoppler
KNX TP main
line
KNX
Linienkoppler
KNX
Linenkoppler
KNX TP Linie
KNX TP Linie
Raum 101
Raum 102
...
Raum 201
Raum 202
...


KNX TP Backbone
KNX
Bereichskoppler
KNX TP Hauptlinie
KNX
Linienkoppler
KNX
Linienkoppler
KNX TP Linie
KNX TP Linie
Raum 101
Raum 102
...
Raum 201
Raum 202
...

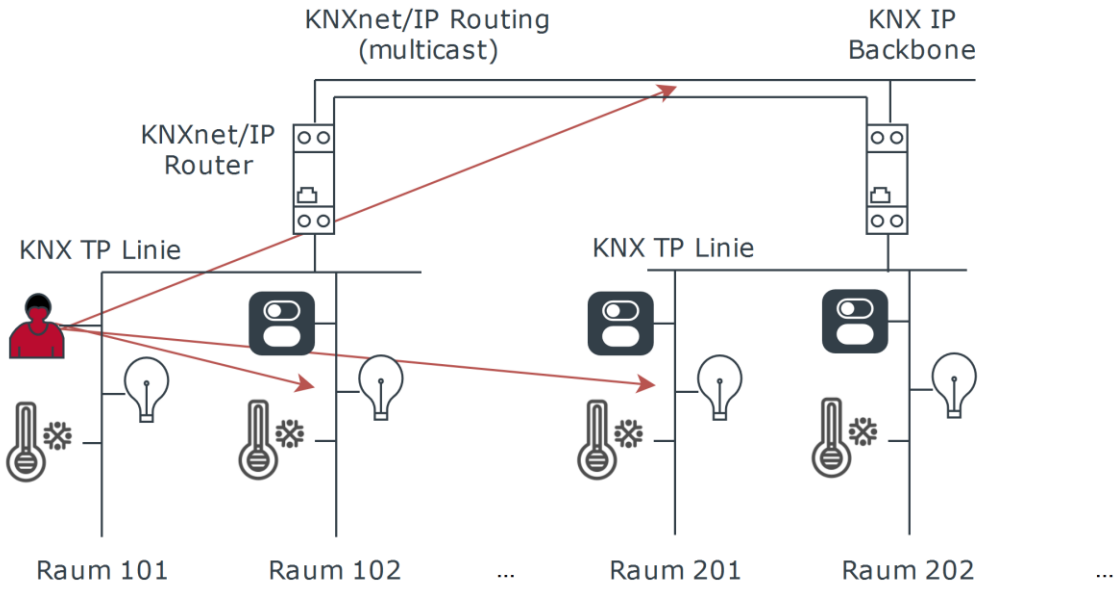
Isolation von Gebäudeautomationsnetzwerken

Beispiel 2: Besser, aber immer noch unsicher

Eine weitere, bessere Möglichkeit ist die Verwendung von KNXnet/IP Routern, wie in der nachfolgenden Grafik dargestellt.

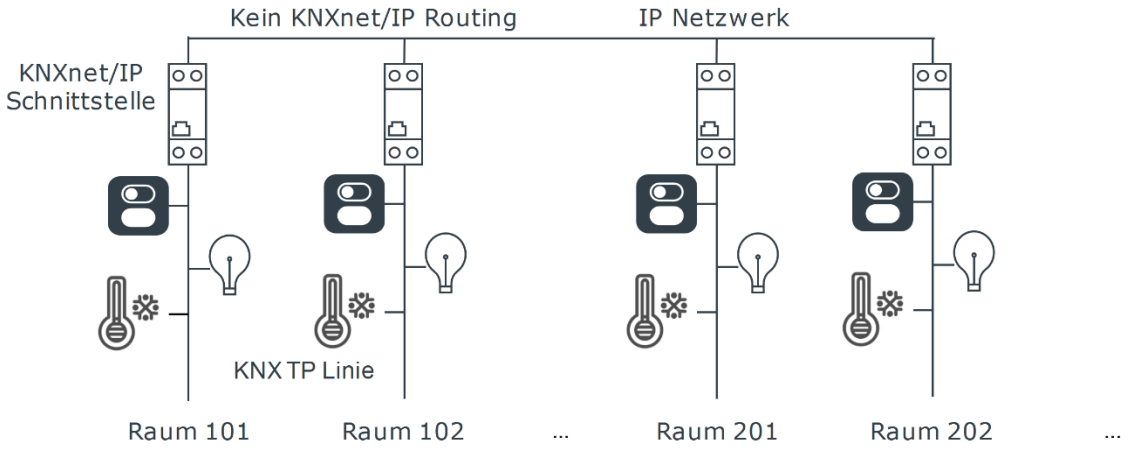


Allerdings kann auch in diesem Fall ein Angreifer über unbefugten Netzzugriff Einfluss auf das gesamte KNX Netzwerk nehmen. KNXnet/IP Router verfügen zwar über Filtermöglichkeiten, aber auch hier sind diese nur bedingt einsetzbar.

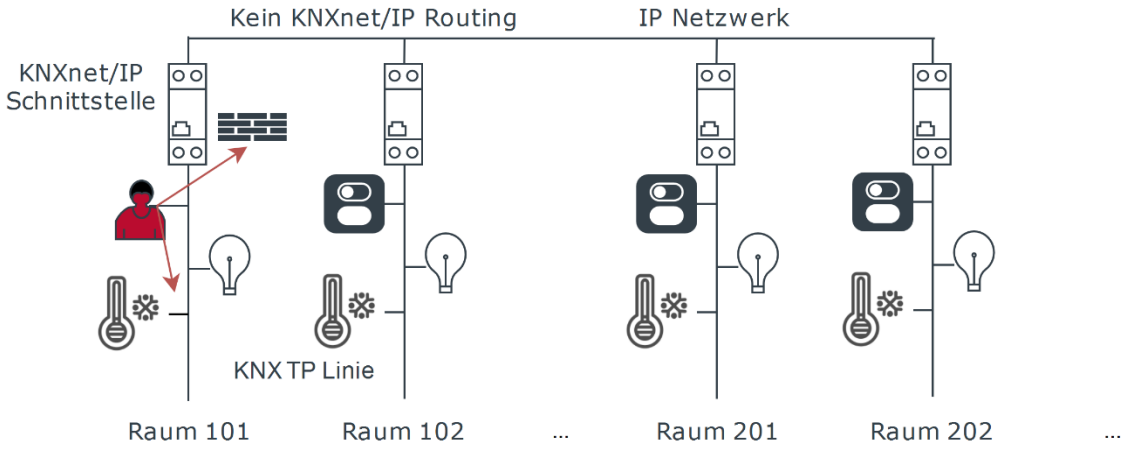


Beispiel 3: Security durch isolierte Räume

Während die beiden vorigen Beispiele keine vollständige Security gewährleisten konnten, bietet dieses Szenario eine erhebliche Minimierung der Sicherheitslücken. Pro Zimmer wird ein eigene KNX Linie verwendet. Um diese über ein übergeordnetes Managementsystem (z.B. Visualisierung) anzubinden, werden KNXnet/IP Schnittstellen verwendet.



Da eine KNX Kommunikation zwischen den einzelnen Räumen nicht notwendig ist, kann man auf KNXnet/IP Routing verzichten. Daher empfiehlt es sich das KNXnet/IP Routing in den KNXnet/IP Routern zu deaktivieren. Alternativ können die weitaus günstigeren KNXnet/IP Schnittstellen verwendet werden. Ein Angreifer ist somit auf die Geräte des gehackten Raumes beschränkt, wodurch ihm keinen Vorteil entsteht, da er ohnehin Zugriff auf seine Raumfunktion hat. Eine Gefahr für das restliche System besteht dabei nicht, da der Angreifer sozusagen isoliert ist.



Doch wie geht man mit zentralen Befehlen wie etwa der Änderung des Sollwerts um, wenn die KNX Kommunikation zwischen den einzelnen Räumen fehlt? Die Lösung liegt in der Verwendung von ausgereifter Gebäudeautomationssoftware.

Teil 1: Aktueller Stand der Security in der Gebäudeautomation

Teil 3: Sichere Gebäudeautomatisierung durch Managementlösung (NETx BMS Server)