KNX NATIONAL SWISS

SICHERE GEBÄUDEINFORMATIK GEBÄUDETECHNIK

KNX SWISS Leitfaden für die Sicherheit der
Gebäude- und Raumautomation mit KNX und IP-Netzwerken

Hinweise

Technische Angaben
Die in dieser Broschüre publizierten Informationen und Angaben wurden nach bestem Wissen und Gewissen erstellt. Irrtümer und technische Änderungen bleiben vorbehalten.

Haftungsausschluss
KNX Swiss haftet nicht für Schäden, die durch die Anwendung der vorliegenden Publikation entstehen können. Jegliche Haftung für Schäden, die direkt oder indirekt aus der Benutzung der in diesem Dokument enthaltenen Informationen entstehen, wird abgelehnt.

Das Dokument ist als PDF unter folgender Adresse verfügbar:
www.knx.ch/secure

Inhalt

Version 1.3 | 01/2025

1 Sinn und Zweck des Dokuments

1.1 Ausgangslage

Smarte Gebäude, die ihre Energie selbstständig regulieren, in ein grösseres Energiesystem eingebunden sind, mit dem Smartphone der Raumnutzerinnen und -nutzer kommunizieren oder gar Daten mit anderen Gebäuden austauschen, sind der Schlüssel zu einer intelligenteren Zukunft des Gebäudeparks in der Schweiz und eine Plattform für die voranschreitende Digitalisierung und Nachhaltigkeit von Wirtschaft und Gesellschaft.

Digitalisierung und Vernetzung ermöglichen Automatisierung. Die damit verbundenen neuen Möglichkeiten, neue Zugriffe von und nach aussen und der Einsatz von künstlicher Intelligenz schaffen aber auch neue Angriffsflächen. Die digitale Kriminalität nutzt diese gerne aus. Das Risiko eines Datenverlusts, einer Erpressung oder der Spionage nimmt zu, wenn das Internet-Protokoll (IP) im Gebäudenetzwerk bestimmend wird. Über Angriffe auf IP-Netzwerke können die Sicherheitsfunktionen der Gebäudeautomation ausgehebelt werden.

Es ist deshalb Zeit, der IT-Infrastruktur der Gebäudeautomation die entsprechende Aufmerksamkeit zu schenken und neue Anlagen sicher zu planen und zu realisieren.

1.2 Ziel des Dokuments

Der vorliegende Ratgeber zeigt Planern, Systemintegratorinnen und Gebäudeinformatikern, wie ein sicheres Gebäudenetzwerk aufgebaut, strukturiert und betrieben werden kann. Zudem liefert er Informationen zu den Zuständigkeiten der IT-Spezialisten der Bauherrschaft, der Planerinnen, Integratoren und Betreiberinnen. Und schliesslich gibt er Hinweise und Tipps, wie ein KNX Secure-Projekt umgesetzt werden kann.

Dieser Ratgeber enthält allgemeine Informationen. Massnahmen müssen individuell an die Gegebenheiten vor Ort angepasst werden.

2 Smart Buildings: die Treiber in der Schweiz

Die Digitalisierung des Schweizer Gebäudeparks steht erst am Anfang. Doch der Druck steigt, neue Gebäude schon intelligent zu konzipieren und bestehende nachzurüsten. Das Internet of Things (IoT) und weitere Treiber verstärken die Entwicklung:

- **Kostendruck:** Mit nur einem Netzwerk im Gebäude vereinfacht sich die Wartung und die Kosten sinken.
- **Energieautarkie:** Smarte Gebäude produzieren und nutzen im besten Fall ihre Energie selbst. Dazu bedarf es eines intelligenten Datenaustauschs zwischen den Geräten, sowohl gewerke- als auch gebäudeübergreifend (Sektorkopplung).
- **Industrie 4.0:** Smarte Fabriken brauchen auch Remote-Zugänge. IT und OT (Operational Technology) wachsen zusammen.
- **Smart City:** In diversen Städten und Quartieren entwickeln sich Ansätze für eine Smart City. Vernetzung und neue Technologien sollen Effizienz, Nachhaltigkeit und das Zusammenleben von Menschen stärken.
- **Technologieentwicklung:** Die hybride (Multi-)Cloud wird zum bestimmenden Konzept der IT-Architekturen. Mit künstlicher Intelligenz, Software zur Automatisierung, neuen Sicherheitsansätzen im Netzwerk wie Zero Trust sowie mit zunehmender Sensordichte, schnellen, drahtlosen Zugängen (5G, Wi-Fi6) und smarten IT-Architekturen können Gebäude auf der Basis von offenen Standards in grössere Netzwerkstrukturen integriert werden.

Ein einziges Netzwerk für alle Dienste und Anlagen im Gebäude statt mehrerer parallel betriebener mit unterschiedlichen Standards: Diese Entwicklung erfolgt einerseits aus Kostengründen, vereinfacht aber auch den Unterhalt sowie die Überwachung des Energieverbrauchs im Gebäude.

Alle benötigten Dienste nutzen eine IP-Infrastruktur und müssen sich an die Vorgaben ihres Netzwerks bezüglich Cybersicherheit halten. Dies ermöglicht die langfristige Pflege aus einer Hand (IT-Abteilung) des gesamten Netzwerk-Managements sowie den Erhalt der Cybersicherheits-Zertifikate.

2.1 Grundlegende Spielregeln

Die IT-Abteilung erhält neue Aufgaben: Sie kümmert sich nicht nur um Datenflüsse und Netzwerke, sondern auch um die Netzwerke der Gebäudeautomation. Sie sorgt nicht nur für sichere Zugänge von aussen (Remote), sondern auch für Netzwerkanschlüsse und -strukturen im ganzen Gebäude. Dabei gilt es, **Ethernet** (Kabel) und Wi-Fi 6 sowie 5G intelligent und sicher zu kombinieren.

Handelt es sich bei einem Gebäude um sogenannte «kritische Infrastruktur», steigen die Anforderungen an die Cybersicherheit. Die Vorgaben der IT werden strenger, auch bezüglich der Geräte.

Ethernet Ein Standard für die kabelgebundene Datenübertragung. Die Technik wurde für LAN (Local Area Networks) erfunden, inzwischen wird sie auch für Wide Area Networks (WAN) verwendet. Für Anwendungen mit hohen Anforderungen an die Zuverlässigkeit kommt Echtzeit-Ethernet zum Einsatz. Derzeit sind Bandbreiten bis 400 Gb/s verfügbar. Der Hunger wächst. 800 Gb/s stehen vor der Tür. Bis zu 1,6 Terabit/s sind in Entwicklung.

3 IT für smarte Gebäude

3.1 Aufbau einer sicheren IP-Infrastruktur

Informationstechnologien basieren auf dem Austausch von Daten – heute auf Basis des Internetprotokolls. Dieses findet sich überall, in lokalen Netzwerken (LAN), in Weitverkehrsnetzen (WAN) sowie im öffentlichen Internet.

Lokale, abgeschottete Geräte, Speicher oder Daten gibt es immer weniger. Die IT entwickelt sich in Richtung einer Cloud-Architektur, die mehrere Anbieter sowie öffentliche und private Clouds zusammenfasst (Multicloud). Hinzu kommen Vorort-IT-Strukturen und Daten, die etwa aus rechtlichen Gründen nicht in der Cloud liegen dürfen. Weiter bilden sich Infrastrukturen «an der Edge», an der Grenze von Netzwerken. In ihnen werden Daten dezentral verarbeitet, dort, wo sie gebraucht werden. Eine kurze **Latenz** ist wichtig.

Latenz Die Verzögerungs- oder Antwortzeit ist ein wichtiges Qualitätsmerkmal der IP-Infrastruktur und je nach Anwendung unterschiedlich wichtig: je niedriger, desto besser die Benutzererfahrung.

Die IT für smarte Gebäude muss also einige Bedingungen erfüllen. Sie ist eng verbunden mit der Gebäudetechnik und verfügt über Schnittstellen mit KNX-Geräten.

Es gelten folgende Mindestvoraussetzungen für die technische Sicherheit:

- Internetanschluss mit statischer IP-Adresse
- Router des Internetproviders im Bridge-Modus mit Firewall
  - > DHCP eingeschränkt, lokales Netz mit fixer IP-Adresse
  - > Eingeschränkte Zugriffe aus dem WAN
  - > Offene Dienste (Ports) nur auf den für den Betrieb wirklich nötigen Geräten
  - > Remote-Zugriffe nur via VPN (Virtual Private Network)
  - > Nur sichere Passwörter erlauben. Noch besser: Multifaktor-Authentifizierung als Standard bzw. **Zero Trust** implementieren
  - > Öffentliche Wi-Fi-Zugangspunkte und Zugang auf TechNet/Firewalls einschränken

Zero Trust Die klassische Netzwerksicherheit basiert darauf, dass jeder Client nach der Authentifizierung Zugriff auf das Netzwerk erhält und sich darin frei bewegen kann. Mit einer Zero-Trust-Architektur ändert sich das. Hier wird jedem Client, jedem Benutzer und jeder Anwenderin stets misstraut. Der höchst individuelle Ansatz direkt bei den Daten ermöglicht die permanente Kontrolle der Datenflüsse.

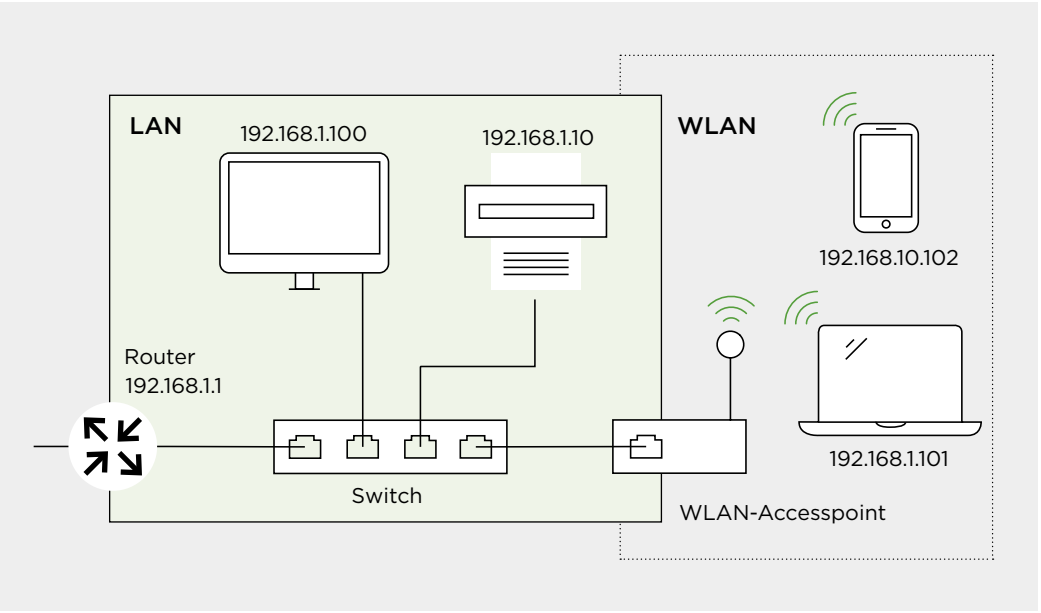


Bild 3.1-1 Aufbau eines einfachen Netzwerks

3.2 Aufbau eines sicheren Netzwerks

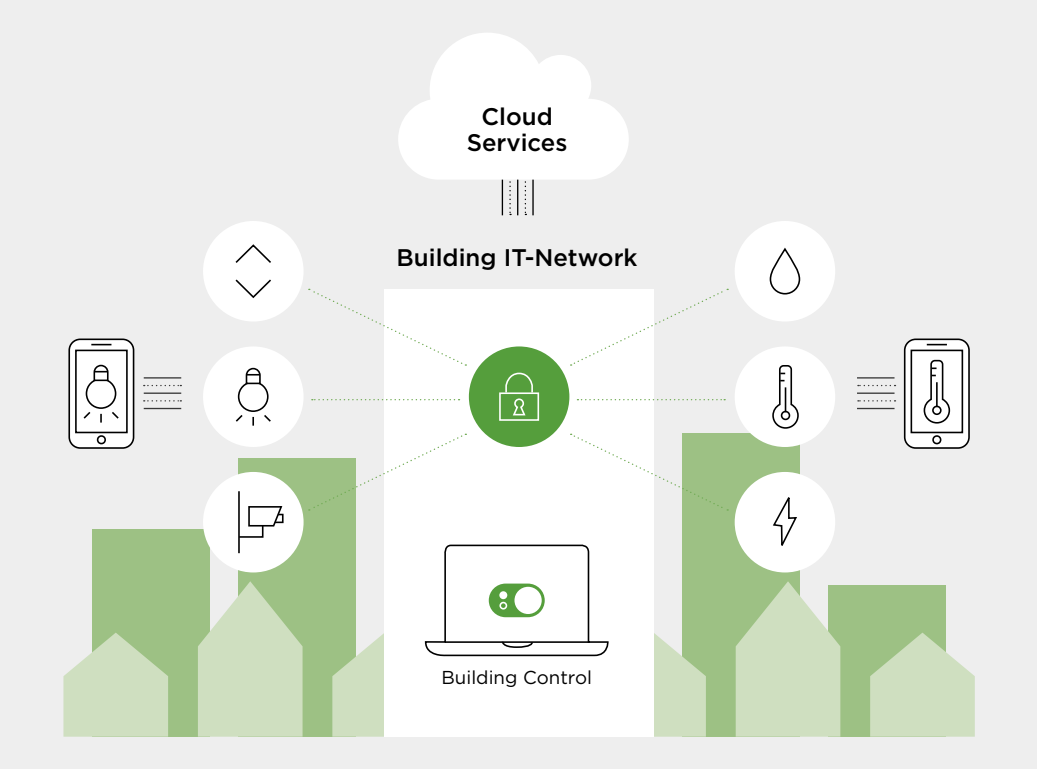
Die Komplexität eines Netzwerks ist nicht zu unterschätzen. Entsprechend wichtig ist beim Aufbau Erfahrung mit Netzwerk-Architekturen. Wer diese nicht hat, braucht die Unterstützung von Netzwerk-Experten. Eine enge Zusammenarbeit mit der IT-Abteilung empfiehlt sich, zumal es hier um den Aufbau einer Private Cloud geht.

Die Private Cloud bietet IT-Services über Internet oder über ein privates Netzwerk für einen beschränkten Nutzerkreis. Das Smart Building ist ein isolierter Teil eines grösseren Netzwerks, das aus weiteren öffentlichen oder privaten Clouds besteht.

Innerhalb des Smart Buildings müssen die unterschiedlichen Anlagen/Anlagenteile über ein gemeinsames, gegen unberechtigten Zugriff gesichertes Netzwerk miteinander kommunizieren können.

Für das smarte Gebäude bedeutet dies, dass die einzelnen «Netzwerk-Silos», wie sie allenfalls in der Vergangenheit geschaffen wurden, nicht mehr dem Stand der Technik entsprechen. Sie bieten zu viele Angriffspunkte, und zudem ist ihre Sicherheit je nach Anlagentyp unterschiedlich geregelt. Im Zuge der Konvergenz von Gebäudeleittechnik und IT empfiehlt deshalb die Marktinteressengruppe **IP-BLiS** die einheitliche Verwendung des Internetprotokolls (IP) im gesamten Netzwerk. IP-BLiS ist keine neue Organisation, sondern eine Vereinigung, in der bestehende Organisationen zusammenarbeiten.

IP-BLis Mehrere Player der Gebäudeautomation arbeiten in der Organisation zusammen, um sichere IP-Netzwerke in Gebäuden zu fördern.



Quelle: ip-blis.org BuildingTrend.png

Bild 3.2-1 IP-BLiS fördert sichere, standardübergreifende und harmonisierte IP-basierte Lösungen im Smart Building.

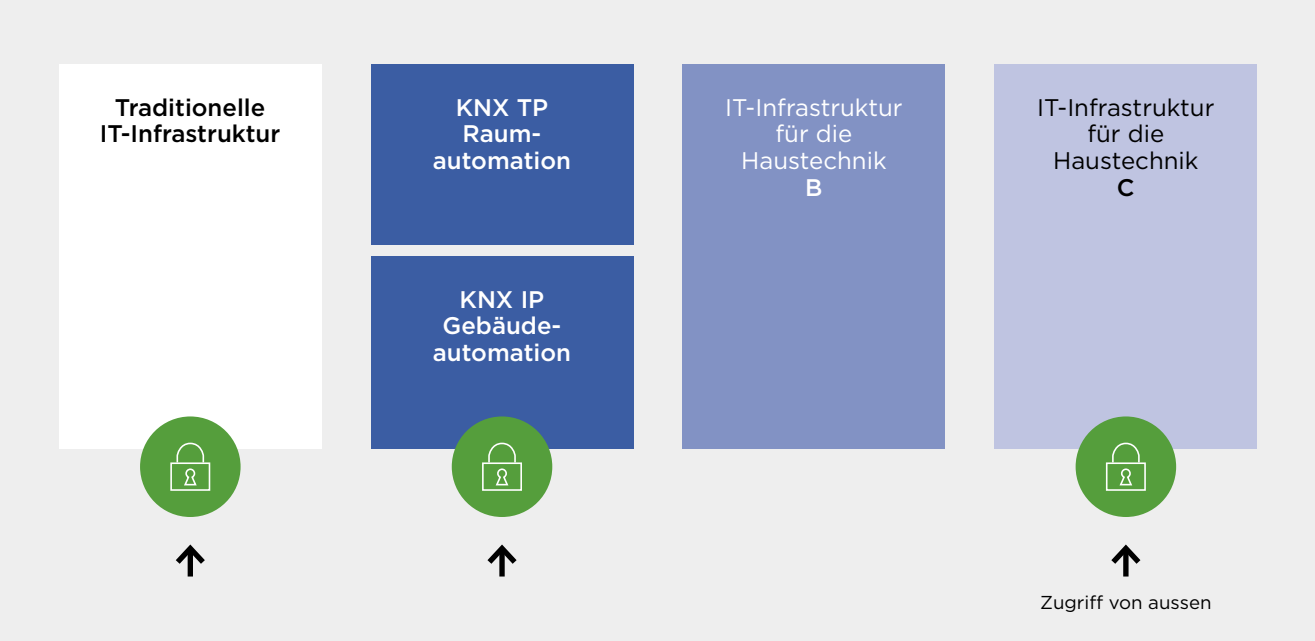


Bild 3.2-2 Eine unübersichtliche Infrastruktur und unterschiedliche Sicherheitskonzepte sind in Gebäuden zu vermeiden.

Stand der Technik ist es, wie in der Einleitung bereits beschrieben, die unterschiedlichen Netzwerke zu einem einheitlichen Netzwerk zusammenzuführen. Dies bedingt, und das liegt in der Natur der Sache, entsprechenden Koordinationsaufwand aller Beteiligten. Ein Netzwerkadministrator kann oder soll bereits in der Projektphase den Aufbau eines solchen Netzwerks einplanen.

Wie können IP-Netzwerke im Gebäude sicher aufgebaut werden?
Jedes Gebäude benötigt einen individuell angepassten Netzwerkaufbau. Grundsätzlich müssen Netzwerke segmentiert, das heisst, in mehrere kleine Subnetzwerke unterteilt werden. Jedes Subnetzwerk kann seine eigenen Schutzvorrichtungen und Kontrollfunktionen erhalten. Wer eindringt, befindet sich erst einmal nur in einem Subnetzwerk.

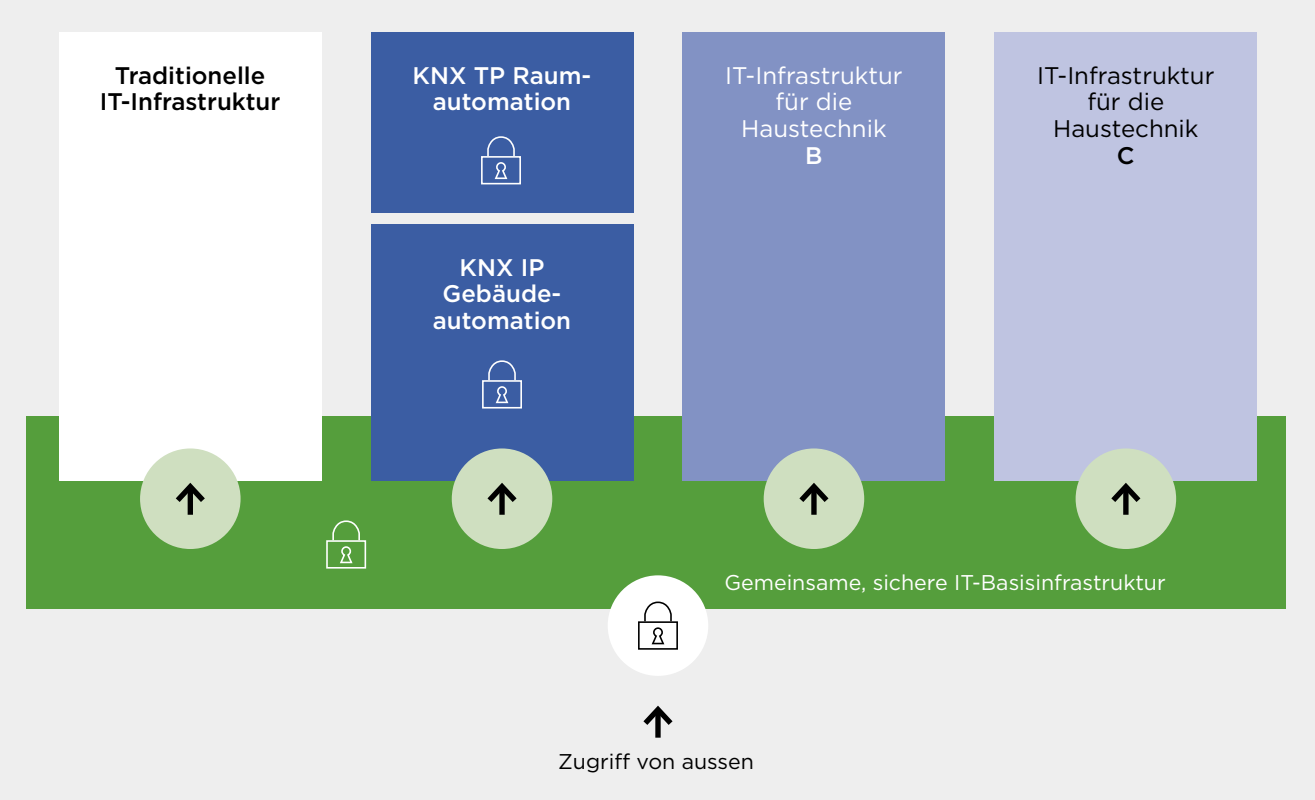


Bild 3.2-3 Es muss eine gemeinsame, sichere und vor allem koordinierte IT-Basisinfrastruktur geschaffen werden.

Netzwerkvirtualisierung ist der nächste Schritt. Mit einem softwaredefinierten Netzwerk (SDN) wird die Kontrolle über das Netz an eine Software abgegeben. Diese steuert alle Netzwerkgeräte zentral. Die einzelnen Router und Switches sorgen nur noch für die Durchleitung und müssen nicht mehr einzeln programmiert werden. Netzwerke lassen sich auch als Service aus der Cloud bereitstellen und zentral managen. **Network as a Service (NasS)** stellt alle benötigten IT-Services bereit, um den Datenverkehr innerhalb des Gebäudes und mit anderen Standorten zentral in der Cloud zu managen.

Mit Netzwerkkonzepten wie **Zero Trust** sichern IT-Teams Gebäude vor unbefugtem Zugriff. Dabei wird jedem Endgerät prinzipiell das Vertrauen entzogen und der Datenverkehr permanent überprüft. Das passwortlose Konzept muss von Anfang an in die Netzwerkplanung integriert werden. Weiter braucht es für den Zugang eine **Multifaktor-Authentifizierung**, das heisst Freigaben über einen zweiten oder gar dritten Kanal (z. B. SMS).

Wie arbeiten wir mit der IT-Abteilung zusammen?
Sie muss frühzeitig involviert werden und eine Netzwerkanalyse durchführen. Diese bestimmt das weitere Vorgehen. Dabei wird untersucht, wer in welcher Rolle auf welche Funktionen und Daten zugreifen können muss. Sinnvollerweise übernimmt die IT auch das Monitoring der Gebäudeautomation bzw. des damit verbundenen Netzwerks. So werden Eindringlinge aufgrund von Anomalien im Netzwerkverkehr automatisch erkannt.

Was ist weiter zu beachten?
Der Perimeter eines Gebäudes ist heute sehr unscharf. Es gibt kein Drinnen oder Draussen mehr. Auch Facility Manager greifen manchmal von ausserhalb des Gebäudes auf gewisse Netzwerke zu – das erhöht die Anforderungen an die Netzwerksicherheit.

SDN bietet die Basis für die Integration weiterer Standorte wie zum Beispiel anderer Gebäude oder Home Offices in ein gemeinsames Netz.

Ethernet-Geräte wie Switches und Router müssen höchste Anforderungen erfüllen und für den Betrieb in SDN geeignet sein. Für kritische Infrastrukturen bietet die Industrie speziell sichere Hardware an.

Ethernet ist die Technik, auf der kabelgebundene Netzwerke und Netzwerkprotokolle wie **IP (Internet Protocol)** basieren. Ethernet überträgt auch Strom, beispielsweise für den Betrieb von Sensoren. Diese Geräte müssen mit Überspannungsschutz versehen sein (SP, Surge Protection). Für Anwendungen in der Automatisierung wird Echtzeit-Ethernet eingesetzt. Die technischen Anpassungen sorgen dafür, dass solche Netzwerke höchste Anforderungen an die Zuverlässigkeit der Kommunikation erfüllen.

Internet-Protokoll
Das Internet Protocol (IP) bildet die Grundlage des Internets und heute der meisten Datennetzwerke. Datenpakete werden unabhängig von einer Verbindung behandelt. IP-Netze sind dynamisch und heterogen und somit relativ ausfallsicher. Im Einsatz sind derzeit IPv4 und IPv6.

Beim **Edge Computing** werden Daten vor Ort und nicht in einem Rechenzentrum verarbeitet – zum Beispiel im neu mit IT ausgerüsteten Gebäude. Das verkürzt die Latenzzeiten etwa für Roboter, die Echtzeitdaten brauchen. Hohe Latenzzeiten würden auch die Datenrisiken in der Automation erhöhen.

Moderne Switches bringen Industrie- und OT-Systeme (Operational Technology) besser unter ein gemeinsames Dach mit den klassischen Computernetzen und führen erprobte Enterprise-Netzwerktechniken auch im Gebäude ein.

Drahtlose Netzwerke (WLAN auf der Basis des Wi-Fi-Standards sowie 5G über Mobilfunk) gilt es ebenfalls in die Überlegungen und Planungen der Gebäudeautomation mit einzubeziehen. Dazu braucht es eine Vermessung des Gebäudes und eine sorgfältige Auslegung der Zugangspunkte mit ihren Reichweiten («Ausleuchtung»).

4 Sicherer Aufbau der Gebäudeautomation (KNX Secure)

4.1 KNX Secure

KNX Secure beinhaltet Technologien zum sicheren Betrieb von KNX-Systemen und zur optimalen Vernetzung mit IP-Netzwerken. Diese Technologien sorgen für sichere KNX-Installationen in der Raum- und Gebäudeautomation – vollumfänglich oder bezogen auf spezifische Anwendungen.

KNX Secure ist für KNX-Systemintegratoren nichts grundlegend Neues. KNX Secure umfasst:

- **KNX IP Secure:** Der KNX-Datenfluss ist durch die vollständige Verschlüsselung im IP-Netzwerk geschützt.
- **KNX Data Secure:** Der KNX-Datenfluss ist durch die Verschlüsselung und Authentifizierung auf dem zweiadrigen KNX-Datenkabel oder über Funk geschützt.

Beide Technologien können kombiniert oder parallel eingesetzt werden.

KNX Secure-Geräte sind mit dem Buchstaben «X», einem Schloss oder einem Schild gekennzeichnet. Sie können gesichert oder ungesichert betrieben werden. Damit bleibt die KNX-Installation bei Änderungen oder Erweiterungen flexibel. Auch der Mischbetrieb ist möglich, eine Umstellung kann auch nach und nach erfolgen, sofern die KNX-Geräte den KNX Secure-Standard unterstützen.

> KNX Secure sollte beim Einkauf neuer Geräte zum Standard werden, insbesondere wenn die Topologie auf IP basiert.

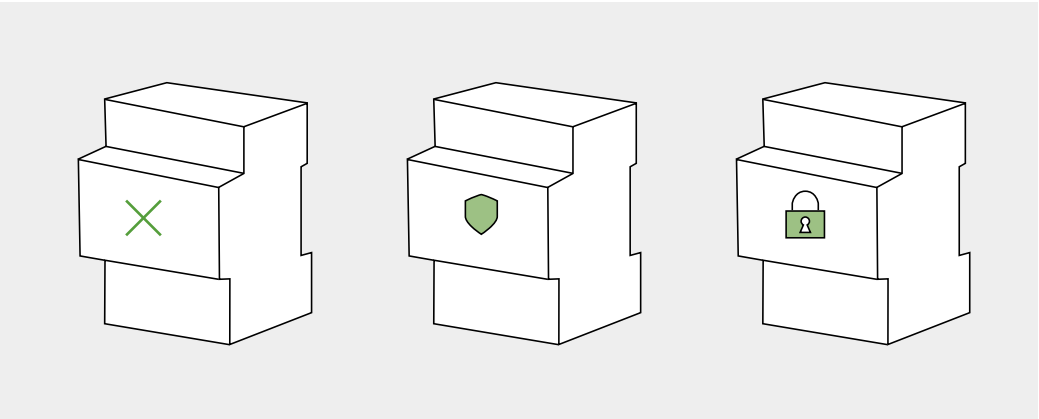


Bild 4.1-1 KNX Secure-Geräte sind unterschiedlich gekennzeichnet.

Aufgrund des längeren Telegrammformats müssen die verwendeten Systemkomponenten (z. B. Bereichs-/Linienkoppler) und die lokalen Datenschnittstellen der ETS (z. B. USB) Extended Frames unterstützen.

4.1.1 Gerätezertifikate

KNX Secure-Geräte verfügen über ein Gerätezertifikat, das in Form eines QR-Codes auf jedem Secure-Gerät aufgebracht ist.

Bild 4.1-2 Beispiel eines Gerätezertifikats auf einem Linienkoppler. Ein Gerätezertifikat ❶ ist fix auf dem Gerät angebracht, das zweite ❷ kann während der Projektierung, vor dem Einbau in einen Verteiler, abgenommen werden.

Das Gerätezertifikat beinhaltet den einmaligen «Hersteller-Initialschlüssel» (Factory Default Setup Key, FDSK, 128 Bit lang) sowie die Seriennummer des Geräts.

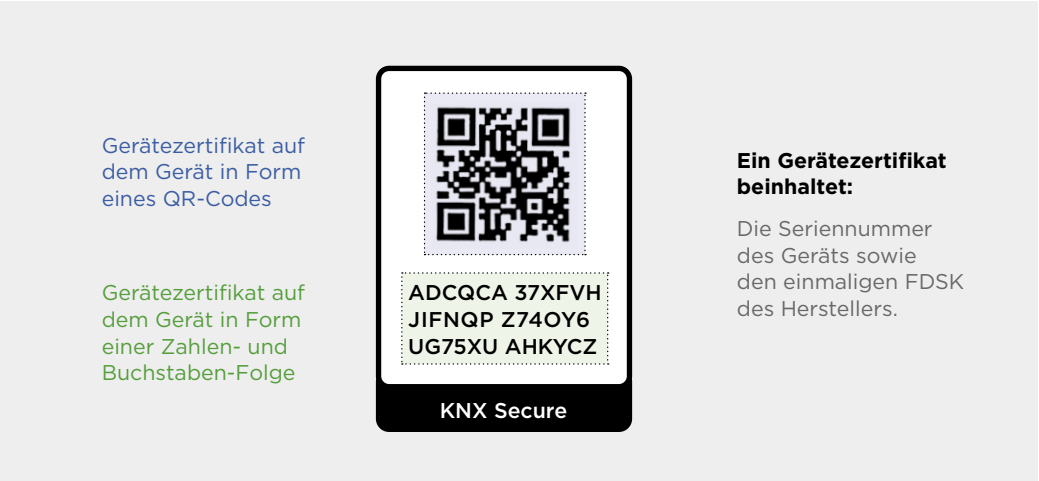


Bild 4.1-3 Das Gerätezertifikat ist auf jedem Secure-Gerät in Form eines QR-Codes oder/und in Form einer Zahlen- und Buchstaben-Folge angebracht. Es beinhaltet den einmaligen «Hersteller-Initialschlüssel» (Factory Default Setup Key, FDSK) sowie die Seriennummer des Geräts.

Es wird empfohlen, das Gerätezertifikat vom Produkt zu entfernen, nachdem es in die ETS gescannt wurde, und es an einem sicheren Ort aufzubewahren (z. B. in der Dokumentation zur Installation).

4.1.2 ETS Handling

ETS Die ETS ist das einheitliche Konfigurationstool, mit dem die Geräte von mehr als 500 Herstellern aus der ganzen Welt parametriert und KNX-Projekte realisiert werden können.

Die Gerätezertifikate, die auf den Secure-Geräten angebracht sind, müssen während der Projektierung in das entsprechende **ETS**-Projekt übernommen werden. Dies kann mit Hilfe eines Scanners, der Kamera am Notebook, über die Eingabe mit der Tastatur oder über eine spezielle App geschehen. Im ETS-Projekt ist bei den KNX Secure-Geräten die Secure-Funktion automatisch aktiviert. Die ETS übernimmt das komplette Handling der Gerätezertifikate für das jeweilige Projekt im Hintergrund.

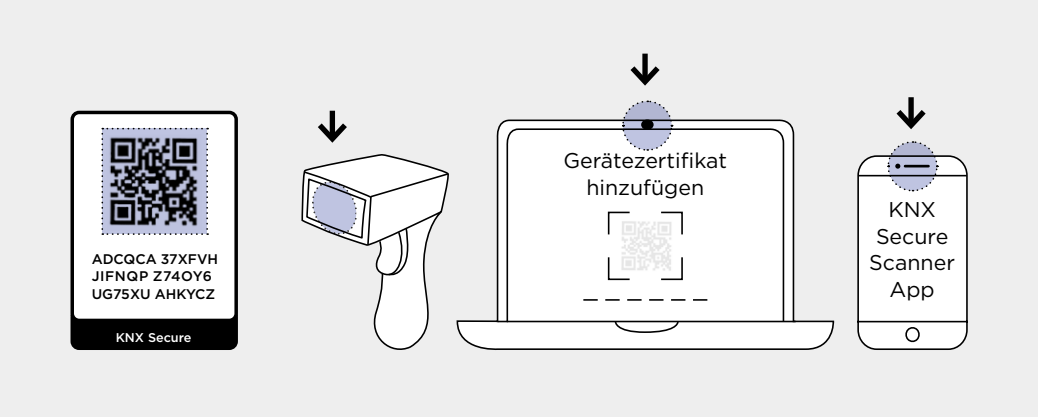


Bild 4.1-4 Die Gerätezertifikate können mit Hilfe eines Scanners, der Kamera am Notebook, über eine spezielle App oder über die Tastatur eingelesen werden.

FDSK Einmaliger «Hersteller-Initialschlüssel» (Factory Default Setup Key, FDSK). Dieser werkseitig voreingestellte Setup-Schlüssel ist pro Gerät eindeutig und lässt sich nicht löschen oder ändern.

Die ETS erkennt beim Laden der physikalischen Adressen der KNX-Geräte anhand ihrer Seriennummern, welcher eingelesene **FDSK** zum jeweiligen Gerät passt. Aus dem FDSK erzeugt sie im Projekt pro KNX-Gerät im Hintergrund einen individuellen, sicheren Geräteschlüssel (Toolkey), der bei der Erstinbetriebnahme an das KNX Secure-Gerät übertragen wird. Dies geschieht beim ersten Download verschlüsselt mit Hilfe des FDSK. Änderungen an einem KNX Secure-Gerät können fortan nur noch mit diesem ETS-Projekt gemacht werden. Der FDSK wird nicht mehr benötigt, es sei denn, das Gerät wird in den Auslieferzustand zurückgesetzt (mittels herstellerspezifischer Mechanismen). Dabei werden alle eingestellten sicherheitsrelevanten Daten gelöscht.

Für jede gesicherte Gruppenadresse, die mit einem KNX Secure-Gerät verbunden ist und die während der Planung generiert wurde, erzeugt die ETS einen geheimen Laufzeitschlüssel. Alle diese Laufzeitschlüssel sind im Projekt gespeichert und im Report «Projekt-Sicherheit» sichtbar (siehe Abschnitt 4.1.4).

Dies funktioniert für alle drahtgebundenen (TP), funkbasierten (RF) und netzwerkbasierten (IP) Geräte.

4.1.3 Darstellung KNX Secure in der ETS

KNX Secure-Geräte sind in der Topologie-Ansicht mit einem blauen Schildsymbol gekennzeichnet, so dass sie leicht von nicht-gesicherten KNX-Geräten zu unterscheiden sind. Mit demselben Schildsymbol sind Gruppenobjekte bzw. Gruppenadressen markiert, die über eine sichere Zuordnung miteinander verbunden sind.

4.1.4 Projektpasswort

Sobald in einem KNX-Projekt in der ETS ein KNX Secure-Gerät eingefügt wird, verlangt die ETS-Software, dass ein Projektpasswort gesetzt wird. Dieses gilt es zu notieren, und es darf **nicht** verloren gehen, da sonst der Zugriff auf das Projekt nicht mehr möglich ist.

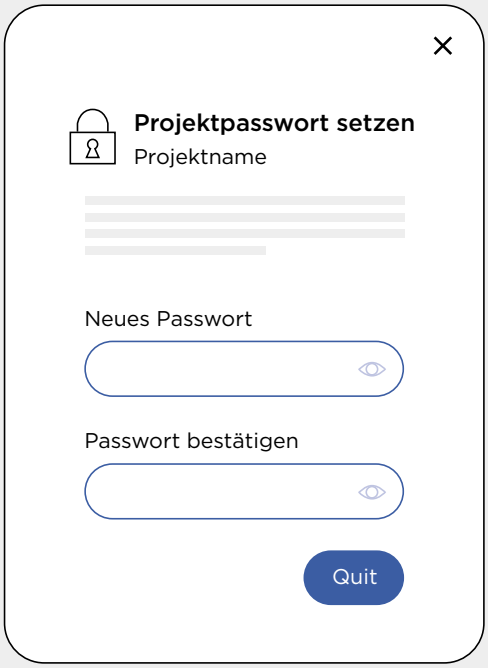


Bild 4.1-5 Das Projektpasswort der ETS muss sicher aufbewahrt werden, da das Projekt ohne dieses Passwort nicht wieder hergestellt werden kann.

4.1.5 Secure Report der ETS

Über das Menü «Reports» in der ETS, und dort via Ansicht «Projekt-Sicherheit», besteht die Möglichkeit, alle Details zur Projekt-Sicherheit des jeweiligen ETS-Projekts auszudrucken. Im Report «Projekt-Sicherheit» sind der Backbone-Schlüssel sowie alle Geräteschlüssel und bei Schnittstellen die Authentifizierungs-Codes aufgeführt. Der Report enthält somit sicherheitsrelevante Daten und sollte geschützt aufbewahrt werden. Sollte das ETS-Projekt verloren gehen, sind diese Informationen zumindest über die Dokumentation verfügbar. Sie werden gebraucht, um die Geräte nach dem Zurücksetzen neu in Betrieb nehmen zu können. Der Report «Projekt-Sicherheit» muss dem Gebäudebetreiber (Auftraggeber) zusammen mit den restlichen Projektdaten übergeben werden.

4.1.6 Normierte Spezifikation

ISO-Standards
iso.org

Die spezifizierten Schutzmechanismen von KNX Secure basieren auf international nach **ISO** 18033-3 normierten Sicherheitsalgorithmen und verwenden die anerkannte Verschlüsselung nach AES 128 CCM.

KNX
knx.org

KNX Secure ist zudem in Europa (als Teil der EN 50090-Reihe, Teil 3-4) und weltweit standardisiert (als EN ISO 22510). KNX ist somit das erste Feldbussystem der Welt, das ein herstellerübergreifendes Sicherheitskonzept für intelligente Haus- und Gebäudeanwendungen bietet. Dies bedeutet einen maximalen Datenschutz durch Authentifizierung und Verschlüsselung der Datenkommunikation.

KNX Data Secure verwendet den CCM-Modus mit 128 Bit AES-Verschlüsselung (Datenverschlüsselung «Counter-Mode» mit Integritätssicherung «CBC-MAC-Mode») und symmetrischen Schlüsseln. Ein symmetrischer Schlüssel bedeutet, dass sowohl der Sender für die Verschlüsselung ausgehender Meldungen (Authentifizierung und Integritätssicherung) als auch der oder die Empfänger zur Verifikation und Entschlüsselung der empfangenen Meldungen denselben Schlüssel verwenden.

4.2 KNX Data Secure

KNX Data Secure verschlüsselt und authentifiziert Telegramme von Endgerät zu Endgerät über die KNX-Übertragungswege wie Twisted Pair und Funk. Dazu müssen alle teilnehmenden und zu schützenden Komponenten KNX Data Secure-Geräte sein, unabhängig davon, ob sie via Twisted Pair oder Funk mit dem KNX-Bussystem verbunden sind.

Die ETS stellt sicher, dass gesicherte Gruppenadressen nur noch mit Kommunikationsobjekten (Geräten) verbunden werden, die KNX Data Secure unterstützen. Neben der vollständigen Absicherung kompletter KNX-Bereiche und KNX-Linien lassen sich mit KNX Data Secure auch einzelne, besonders gefährdete KNX-Anwendungen absichern.

In derselben Topologie sind gesicherte und ungesicherte Funktionen parallel möglich – selbst innerhalb eines KNX Data Secure-Geräts. Das bedeutet, dass ein KNX Data Secure-Gerät sowohl Gruppenobjekte haben kann, die mit sicheren Gruppenadressen verbunden sind, als auch solche mit ungesicherten Gruppenadressen.

Bei KNX Data Secure ist unbedingt zu berücksichtigen, dass die auf der Busleitung übertragenen Telegramme wegen des Sicherheitsschlüssels länger sind als Standard-Telegramme. Deshalb muss bereits bei der Planung auf eine sinnvolle Aufteilung der Topologie, insbesondere auf die Anzahl der gesicherten Geräte pro Linie, geachtet werden. Seit ETS 6 sind Segmentkoppler mit Filtertabellen einsetzbar, die dank der aktivierten Filtertabelle den Busverkehr entsprechend segmentieren können.

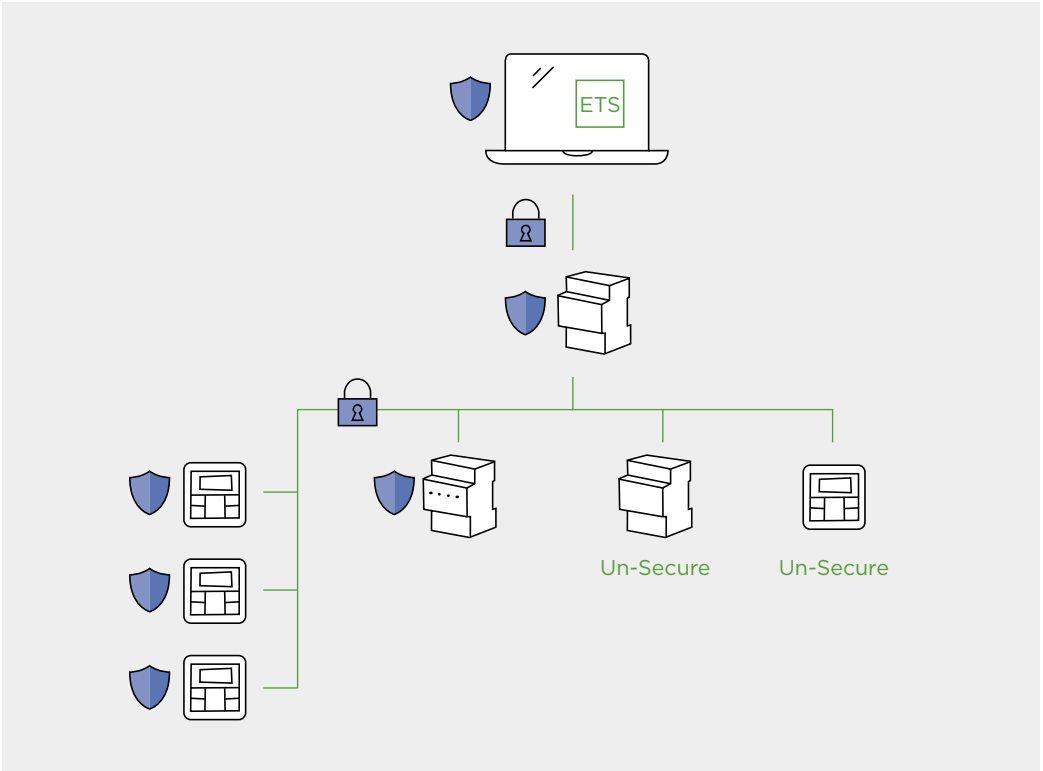


Bild 4.2-1 KNX Data Secure: KNX-Telegramme und -Geräte im KNX-Netzwerk sind verschlüsselt und geschützt. Sie können von unbefugten Dritten im Netzwerk nicht mehr ausgelesen, manipuliert oder verändert werden.

4.3 KNX IP Secure

Mit KNX IP Secure werden alle KNX-Telegramme, welche KNX IP-Router (oder KNX IP-Geräte) in einem Projekt untereinander austauschen, verschlüsselt und gesichert übertragen. KNX-Tunneling- oder -Routingmeldungen auf IP können dadurch durch Dritte nicht mitgelesen oder manipuliert werden, siehe auch Abbildung 6.2-1 «Prinzipieller Aufbau eines sicheren Gebäudetechnik-Netzwerks». Die **ETS** bereitet die IP-Kommunikation der KNX IP-Router bei der Konfiguration des Projekts im Hintergrund für die Verschlüsselung entsprechend vor.

ETS Mit der Engineering Tool Software ETS werden KNX-Geräte konfiguriert. Sie ist herstellerneutral.

Die ETS erstellt, bei Aktivierung der «Sicheren Inbetriebnahme» beim KNX IP-Router, im Hintergrund einen «Backbone-Schlüssel». Dieser kann bei Bedarf in der ETS über das Menü «Reports» > «Projekt-Sicherheit» jederzeit abgerufen werden. Dritte, also Geräte, Systeme und Gateways, die nicht mit der Projekt-ETS konfiguriert wurden, können mit Hilfe dieses «Backbone-Schlüssels» an der gesicherten Kommunikation teilnehmen.

Wird die Einstellung «Sichere Inbetriebnahme» in der ETS nach einer Aktivierung deaktiviert und später wieder aktiviert, generiert die ETS bei jeder Aktivierung einen neuen Backbone-Schlüssel. Dieser muss dann in allen Geräten, die mit dem KNX IP-Backbone kommunizieren, wieder angepasst werden.

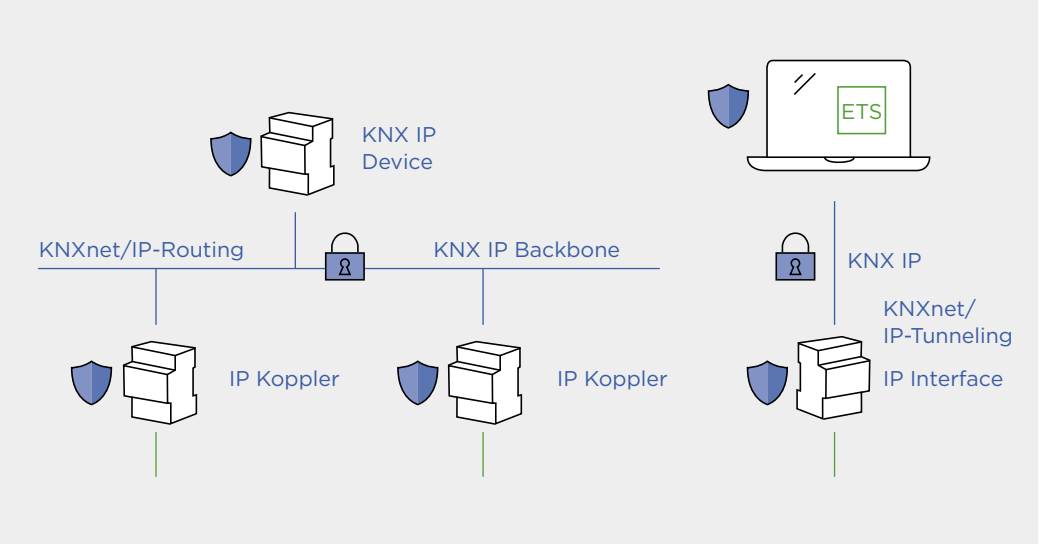


Bild 4.3-1 KNX IP Secure: KNX-Telegramme im IP-Netzwerk (sowohl KNXnet/IP-Routing als auch KNXnet/IP-Tunneling) sind verschlüsselt und geschützt. Sie können von unbefugten Dritten im Netzwerk nicht mehr ausgelesen oder manipuliert werden.

4.3.1 KNX IP-Router

Ein KNX IP-Router (siehe Abb. 4.3-2) besteht aus einer Verbindung zu KNX TP, die über die rot-schwarzen Klemmen zu den KNX TP-Komponenten führt, sowie einer Verbindung zur übergeordneten Linie, die mit Hilfe von IP realisiert ist (RJ-45 Anschluss).

Auf IP-Ebene verfügt der KNX IP-Router über eine Router-Funktion, basierend auf KNXnet/IP-Routing, sowie mehrere Schnittstellen, die auf KNXnet/IP-Tunneling basieren. Für den richtigen Schutz muss KNX Secure zwingend sowohl beim Router als auch bei allen Schnittstellen aktiviert sein.

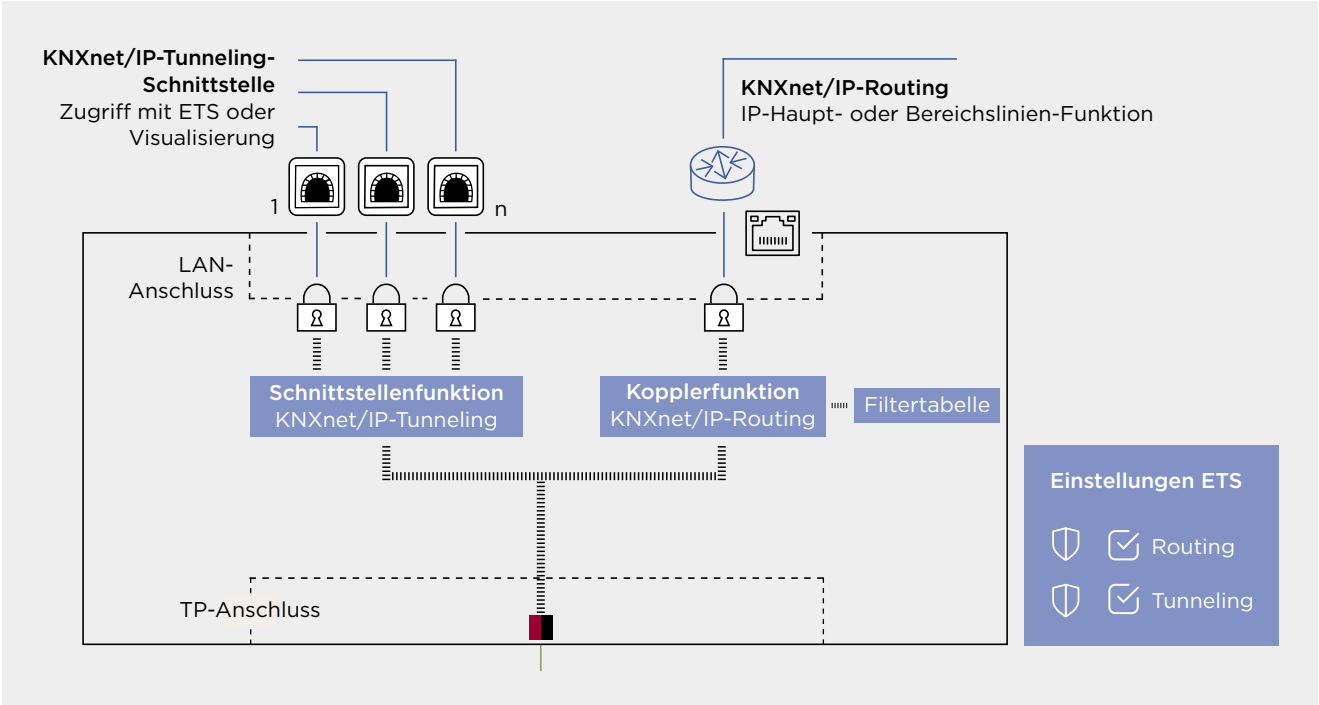


Bild 4.3-2 Aufbau eines KNX-IP-Routers mit seinen drei Schnittstellen: KNXnet/IP-Tunneling, KNXnet/IP-Routing und KNX-Twisted-Pair (TP).

Secure für die Routing-Funktion (KNXnet/IP-Routing)
KNX IP-Routing-Telegramme sind verschlüsselt und können nur von Geräten gelesen werden, die entweder über den Backbone-Schlüssel der ETS verfügen oder mit demselben bzw. in demselben ETS-Projekt konfiguriert wurden. Auch mit der ETS kann via KNXnet/IP-Routing auf die KNX-Anlagen zugegriffen werden. Ist Secure aktiviert, geht dies jedoch nur noch mit dem ETS-Projekt, mit dem der Router konfiguriert wurde.

Secure für IP-Schnittstellenfunktion (KNXnet/IP-Tunneling)
Je nach Hersteller können KNX IP-Router mehrere KNXnet/IP-Tunneling-Schnittstellen haben, die für Visualisierungen oder die Kommunikation mit anderen Anlagen verwendet werden. Nur wenn diese KNXnet/IP-Tunneling-Schnittstellen in der ETS ebenfalls auf KNX Secure geschaltet sind, ist die IP-Kommunikation vollständig sicher konfiguriert. Der Zugriff auf das System ist dann nur noch mit der entsprechenden Projekt-ETS möglich.

4.3.2 KNX IP-Schnittstellen

KNX IP-Schnittstellen werden für Visualisierungen oder die Kommunikation mit anderen Anlagen verwendet. Sie dienen auch als Schnittstelle zur ETS.

Secure für KNX IP-Schnittstellen
KNXnet/IP-Tunneling-Schnittstellen müssen in der ETS auf KNX Secure geschaltet sein. Der Zugriff via IP auf das KNX-System ist dann nur noch mit der Projekt-ETS möglich oder mit einem Gerät (Visualisierung usw.), das den Authentifizierungs-Code der entsprechenden Schnittstelle kennt.

4.4 KNX Secure-Topologien

4.4.1 KNX Data Secure im ganzen Projekt

KNX Secure-Installationen lassen sich dank der durchgehenden KNX Secure-Technologie natürlich auch über ganze KNX TP-Anlagen mit mehreren Bereichen und Linien aufbauen. Auch hier ist es möglich, gesicherte und ungesicherte Geräte in derselben KNX-Topologie zu betreiben.

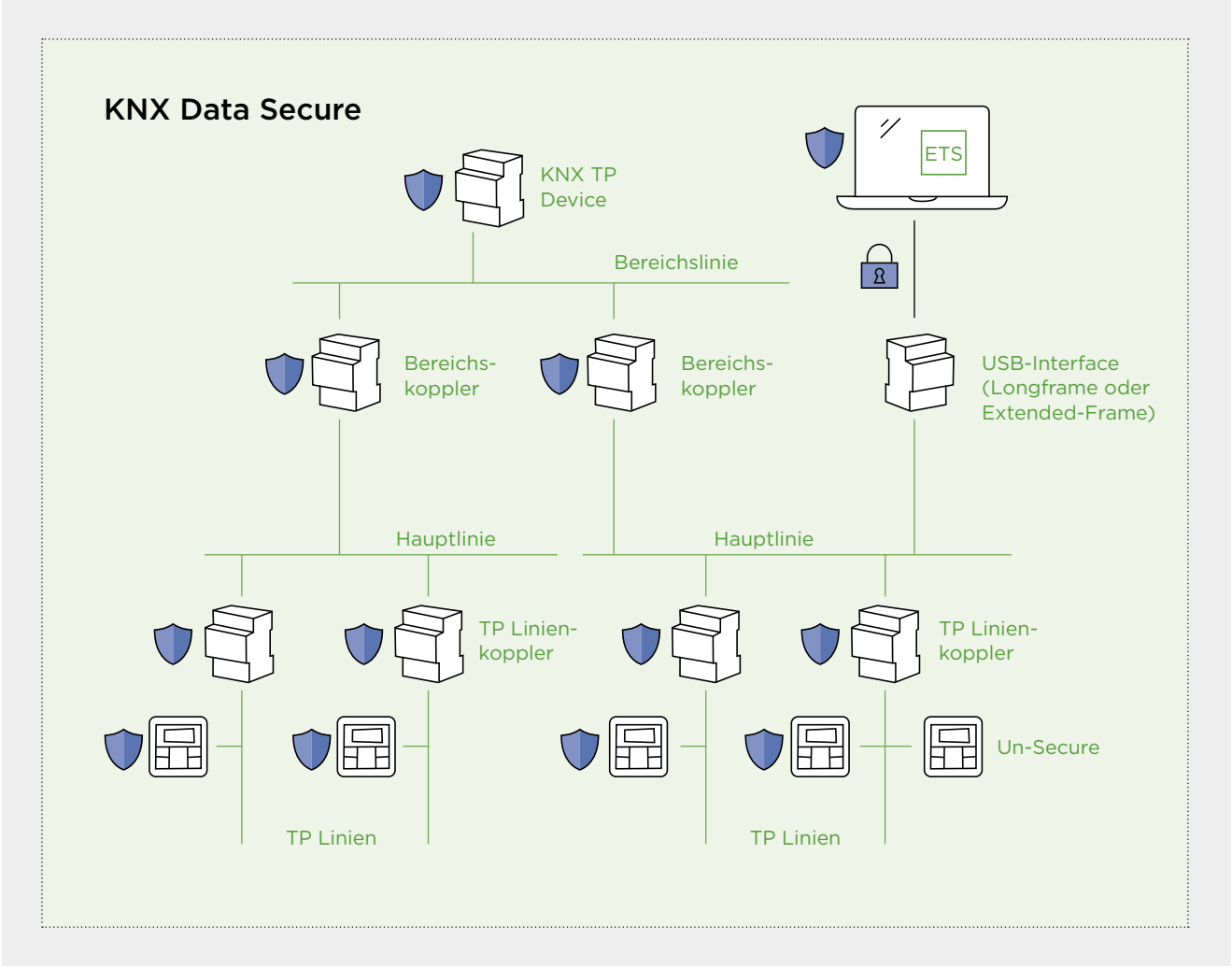


Bild 4.4-1 KNX Data Secure-Projekt über mehrere Linien und Bereiche

4.4.2 KNX Data Secure und KNX IP Secure in Kombination

Dies ist eine Anwendung, die vor allem in grösseren Projekten schnell zum Standard werden sollte. KNX Data Secure und KNX IP Secure können in gemischten IP/TP-Topologien gemeinsam eingesetzt werden. Dank dieser Möglichkeit lassen sich kritische Bereiche bzw. Gebäudeautomations-Anwendungen sehr gut schützen, unabhängig davon, ob sie via IP, Twisted Pair oder gar KNX-Funk erschlossen sind.

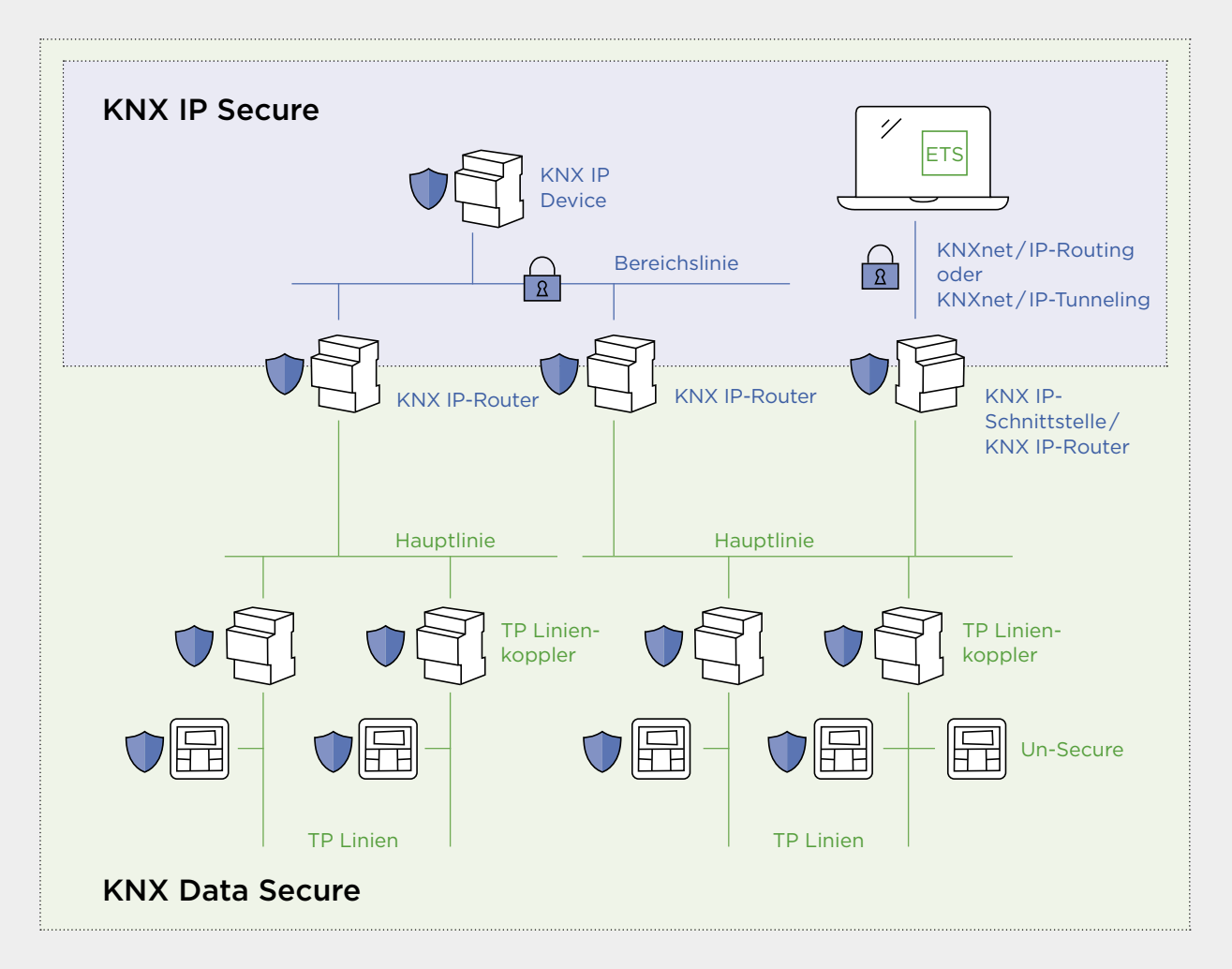


Bild 4.4-2 KNX Data Secure und KNX IP Secure in einem Projekt

4.4.3 Secure Proxy

Secure Proxy Koppler ermöglichen die Kommunikation zwischen Un-Secure-Geräten und Secure-Geräten in demselben Projekt. Sie stellen eine optimale Lösung dar, um bestehende Anlagen durch Hinzufügen von Secure-Geräten zu erweitern, ohne die vorhandenen Un-Secure-Geräte ersetzen zu müssen.

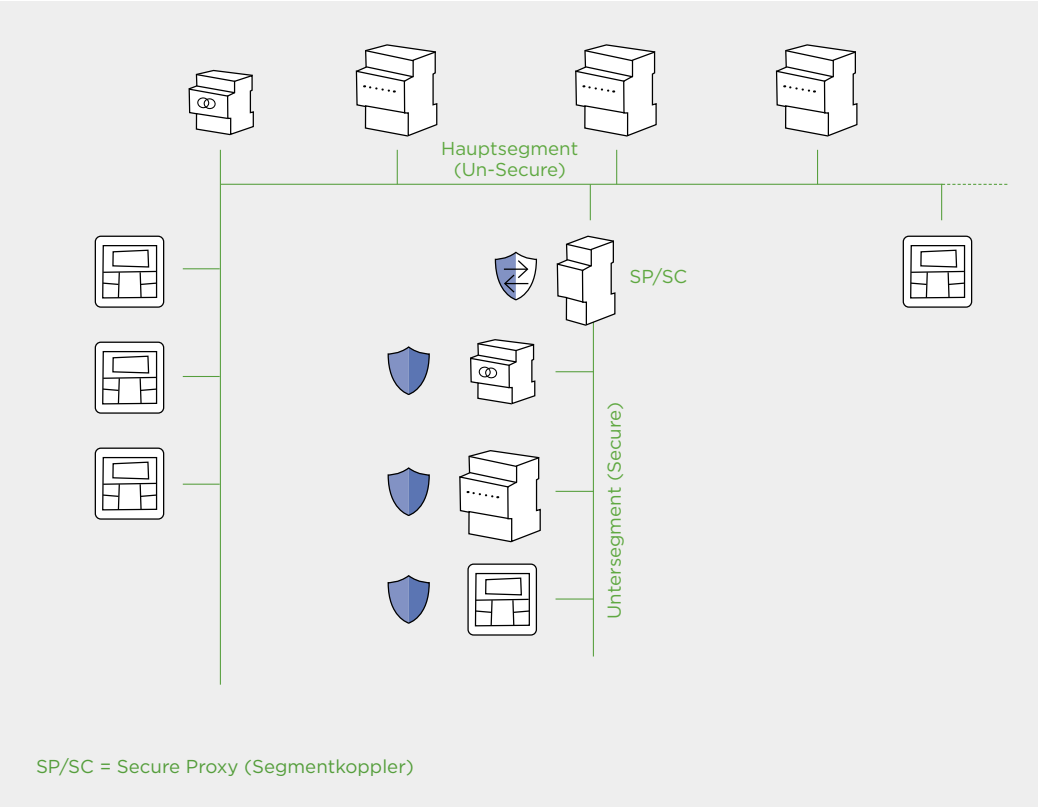


Bild 4.4-3 Secure-Geräte können mit Hilfe eines Secure Proxy in ein KNX-Un-Secure-Projekt eingebunden werden.

4.4.4 KNX IoT-Topologie

KNX IoT nutzt IPv6, verfügt über eine gesicherte Kommunikation und ist eine Erweiterung der bisherigen KNX-Spezifikation bzw. der Übertragungsarten TP, RF oder KNX/netIP. KNX IoT vereinfacht den Zugang für Drittanwender zur KNX-Infrastruktur, die sich seit Jahrzehnten bewährt.

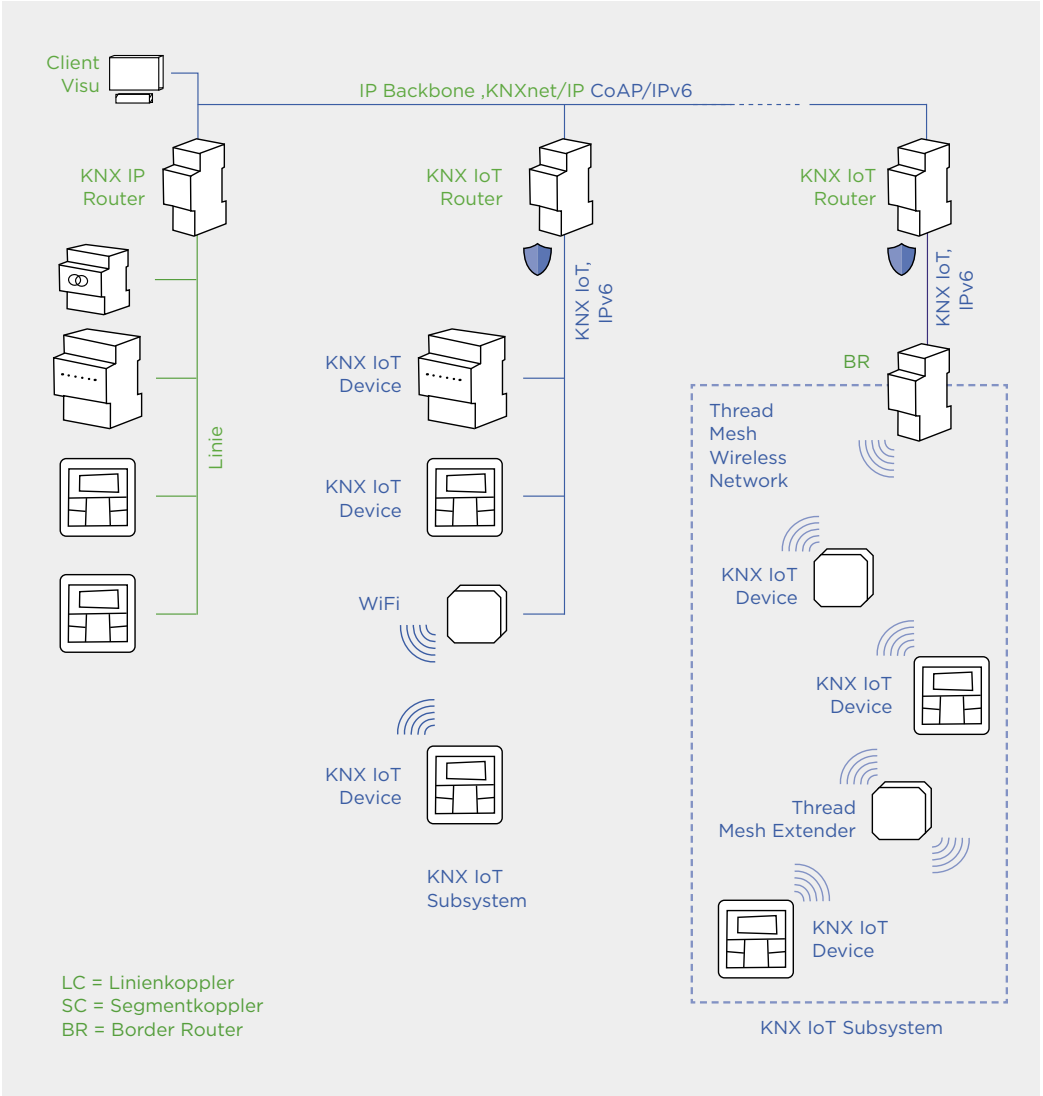


Bild 4.4-4 Prinzipieller Aufbau einer KNX IoT Topologie. Der IPv4-Backbone kann auch für den Transport der KNX-IoT-IPv6-Nachricht verwendet werden.

4.5 Wichtige Begriffe und ihre Definition

Begriffe, die im Umfeld von KNX Data Secure wichtig sind, und ihre Bedeutung

Projektpasswort
Um ein Secure-Gerät mit aktivem Secure-Modus programmieren zu können (oder den Secure-Modus für das Secure-Gerät zu aktivieren oder zu deaktivieren), muss im ETS-Projekt die «Sichere Inbetriebnahme» eingeschaltet werden. Dies ist nur möglich, wenn für das ETS-Projekt vorher ein Projektpasswort vergeben wurde.

Gerätezertifikat
QR-Code auf dem Secure Gerät. Beinhaltet den einmaligen «Hersteller-Initialschlüssel» (Factory Default Setup Key, FDSK) sowie die Seriennummer des Geräts.

Factory Default Setup Key (FDSK)
Der Factory Default Setup Key (FDSK) jedes KNX Data Secure-fähigen Geräts ist weltweit einmalig und wird zu dessen erster Inbetriebnahme verwendet. Er ist 128 Bit lang und als Hersteller-Initialschlüssel eines KNX Data Secure-fähigen Geräts zu verstehen. Der FDSK ist im Gerätezertifikat enthalten.

Seriennummer
Die Seriennummer ist eine 6 Byte lange Identifizierungsnummer des Herstellers zur eindeutigen Kennzeichnung von KNX-Geräten. Sie wird im Zuge der Produktion individuell (weltweit für jeden Hersteller einmalig) festgelegt und unveränderlich in die Geräte programmiert.

Geräteschlüssel, Toolkey
Der Toolkey wird ausschliesslich von der ETS zum Programmieren eines KNX Data Secure-fähigen Geräts verwendet. Er ist ebenfalls 128 Bit lang, eindeutig für jeweils ein Gerät im Projekt und ersetzt bereits bei der ersten Inbetriebnahme den FDSK. Anschliessend verwendet die ETS für jeden Programmiervorgang im gesicherten Betrieb den Toolkey.

Gruppenschlüssel/Laufzeitschlüssel
Um die Laufzeitkommunikation über Gruppenadressen mit Data Secure abzusichern, werden Gruppenschlüssel (Group Keys) für die Ver- und Entschlüsselung von Gruppentelegrammen verwendet. Jede Gruppenadresse besitzt in einem ETS-Projekt einen eigenen, 128 Bit langen Laufzeitschlüssel (AES-Schlüssel), sofern die Adresse zur sicheren Kommunikation zwischen KNX Data Secure-Geräten verwendet wird. Ein Autorisierungscode in den Telegrammen stellt sicher, dass nur die Geräte der entsprechend konfigurierten Gruppe Daten austauschen können.

Backbone-Schlüssel
Ist IP für das Backbone-Medium eines ETS-Projekts gewählt und die Sicherheit des IP-Backbone aktiv, generiert die ETS für das Projekt den Backbone-Schlüssel. Die ETS lädt diesen Key dann in die KNX IP Secure-Koppler und KNX IP Secure-Interfaces des Projekts (falls diese die gesicherte Kommunikation nutzen bzw. die sichere Inbetriebnahme aktiviert haben). Der Backbone Key sowie der Sicherheits-Aktivierungsstatus der Secure-Geräte und Tunneling-Kanäle sind dem Report «Projekt-Sicherheit» zu entnehmen.

Master-Reset
Funktion zum Zurücksetzen eines KNX Secure-fähigen Geräts in einen vom Hersteller definierten Funktionszustand. Beim Ausführen eines Master-Reset werden alle Benutzereinstellungen gelöscht und der initiale Schlüssel (FDSK) wieder aktiviert.

4.6 Zusammenfassung KNX Secure

KNX Secure ist für KNX-Systemintegratoren und -integratorinnen nichts grundlegend Neues, sondern eine Erweiterung der bestehenden KNX-Technologie. KNX Secure beinhaltet Technologien für den sicheren Betrieb von KNX-Systemen über Twisted-Pair (2-Draht-Kabel), Funk oder IP-Netzwerke. Diese Technologien sichern die Raum- und Gebäudeautomation gegen Cyberangriffe – entweder die ganze Anlage oder nur spezifische Anwendungen.

In einem KNX-System (Projekt) können parallel einzelne KNX-Geräte Secure und andere Un-Secure betrieben werden. Auch die Gruppenadressen, über welche die Geräte in einer Anlage miteinander kommunizieren, können sowohl Secure als auch Un-Secure ausgeführt sein. Die Integratoren (Planer) bestimmen anhand der Projekteigenschaften und in Absprache mit der Bauherrschaft, welche KNX-Gruppenadressen und KNX-Geräte Secure ausgeführt und welche konventionell (Un-Secure) belassen werden.

KNX Secure verhindert:

- Dass die Parameter und Einstellungen von KNX Secure-konfigurierten Geräten (Sensoren, Aktoren usw.) mit einer «projektfremden» ETS-Software verändert werden können. Der Zugriff auf diese Geräte ist nur mit dem «Original»-ETS-Projekt möglich, in dem die von der ETS aus dem FDSK erzeugten Geräteschlüssel (Toolkey) hinterlegt sind.
- Dass die KNX-Telegramme, die über KNX Secure gesichert sind, ausgelesen oder manuell bzw. von Dritten auf den Bus gesendet werden können. Ungesicherte Gruppenadressen in einem KNX-System können nach wie vor aufgezeichnet und manipuliert werden, auch wenn Teile des Systems Secure ausgeführt sind (Ausnahme bei KNX IP Secure).
- Dass bei KNX IP Secure KNX-IP-Telegramme ohne Backbone und Projektschlüssel abgehört oder manipuliert werden können. Die komplette KNX-Kommunikation über IP ist mit AES-128 verschlüsselt und mit einem Zeitstempel versehen.

Segmentkoppler können Integratoren helfen, die Topologie eines Projekts KNX Secure-gerecht zu strukturieren. Sie können ein wichtiges Hilfsmittel sein, um den Telegrammverkehr in einzelne Zonen zu unterteilen.

Schnelle Tipps

In einer KNX-Installation können KNX IP Secure und KNX Data Secure parallel eingesetzt werden.

In einer KNX-Anlage können gesicherte und ungesicherte Anwendungen parallel eingesetzt werden. Nicht alle Geräte müssen gesichert sein.

Wenn mehrere IP-Router in einer Anlage eingesetzt werden und einer davon wird auf KNX IP Secure umgestellt, müssen alle anderen auch auf IP Secure umgestellt werden.

Ein Kommunikationsobjekt eines Geräts, das bereits mit einer gesicherten Gruppenadresse verbunden ist, kann nicht mehr mit einer weiteren, nicht gesicherten Gruppenadresse verbunden werden. Ohne Sicherheitsproxys in der Installation gilt diese Regel für die gesamte Installation. Mit einem Sicherheitsproxy gilt die Regel für die relevante Sicherheitsdomäne.

Innerhalb derselben Sicherheitsdomäne muss eine Gruppenadresse entweder einfach oder sicher für alle verbundenen Gruppenobjekte sein. Wenn ein Gerät nicht Secure, Sicherheit aber unverzichtbar ist, muss dieses nicht sichere KNX-Gerät gegen ein KNX Secure-Gerät ausgetauscht werden.

Die neuen Sicherheitsfunktionen können nahtlos auch in bestehende Anlagen integriert werden. KNX Secure ist eine aufwärtskompatible Erweiterung: Bestehende Geräte ignorieren KNX Secure-Nachrichten.

4.7 Ausblick KNX IoT

KNX IoT wird ausschliesslich über IP-Netzwerke eingesetzt und nutzt TLS (Transport Layer Security) zur Absicherung des Datenflusses. Je nachdem, welche API genutzt wird, sind Ethernet, WLAN oder Thread die zur Verfügung stehenden Möglichkeiten. Dadurch ist eine Ende-zu-Ende-Verschlüsselung der Kommunikation von einem Sensor bis in die Cloud möglich.

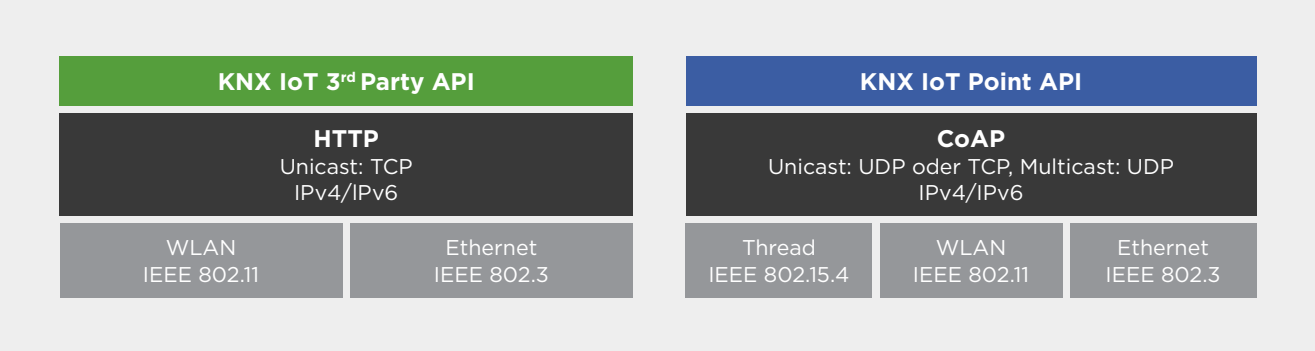


Bild 4.7-1 Beide Varianten von KNX IoT (3rd Party API und Point API) nutzen ausschliesslich Standard IP Netzwerke und halten sich an die IEEE und IETF Standards. Probleme mit IT-Abteilungen bei Kunden können damit zukünftig so gut wie ausgeschlossen werden.

Schnelle Tipps

Besonders zu beachten sind Anlagen in öffentlichen Bereichen, also überall dort, wo sich Personen unbeobachtet bewegen können. Auch verkabelte KNX-Systeme können dort angreifbar sein.

Bei drahtlos kommunizierenden KNX-Anlagen wird der Einsatz von KNX Secure empfohlen.

Ist eine Anlage mit dem Internet verbunden, ist der Einsatz eines VPN-Tunnels für den Zugriff über das Internet ein absolutes MUSS. Beim Einsatz einer KNX Secure-Tunnelschnittstelle ist zu beachten, dass die von der ETS empfohlenen starken Passwörter verwendet und nicht durch eigene schwache Passwörter ersetzt werden.

Bei einem KNX IP-Backbone und anderen IP-Netzwerken muss eine VLAN-Trennung genutzt werden. Das KNX IP-Netzwerk und andere Netzwerke dürfen nur über eine geeignete Firewall miteinander kommunizieren.

Gebäudeautomationsgeräte müssen «IT-freundlich» sein und beispielsweise die dynamische und fixe Vergabe von IP-Adressen (DHCP) sowie die Namensauflösung (DNS) unterstützen. Broadcasts für die Kommunikation werden unterbunden.

5 Cybersecurity im Gebäude und in der Gebäudetechnik

5.1 Grundlagen der Cybersecurity

Das Internet wurde in den 60er-Jahren zwar ausfallsicher gestaltet, doch Sorgen um die Sicherheit der Server und Netzwerke hat man sich nie gemacht. Das war ein Fest für die digitale Kriminalität. Sie hat sich inzwischen zu einem Milliardenbusiness entwickelt, das ökonomisch nicht anders als die legale Wirtschaft funktioniert, mit Anbietern, Zwischenhändlern und mit einem funktionierenden «Kundenservice». Es braucht heute deshalb keine Hackerkenntnisse, um einen Angriff auf ein Unternehmen oder ein Smart Building zu starten, nur die richtigen Kontakte und eine hohe kriminelle Energie. Entsprechend steigt die Zahl der Sicherheitsdurchbrüche laufend. Es ist keine Frage mehr, ob es einen erwischt, sondern nur wann und mit welchen Folgen. Darum sollten solche Angriffe, die so oder so kommen, möglichst rasch erkannt und Gegenmassnahmen ergriffen werden.

Cybersecurity als Disziplin der IT befasst sich mit allen Aspekten der Sicherheit und der Risiken im Umgang mit digitalen Prozessen. Massnahmen, Konzepte und Richtlinien werden entwickelt und umgesetzt, damit mit dem Internet verbundene Geräte und Netzwerke vor unerlaubten Zugriffen, Datendiebstählen und Manipulationen jeder Art geschützt sind.

Eine Cyberattacke ist ein feindlicher Angriff auf ein fremdes IP-Netzwerk und die damit verbundenen Endgeräte. Der Zweck ist unterschiedlich – stark zugenommen haben Ransomware-Angriffe, bei denen Daten verschlüsselt und erst nach Zahlung eines Lösegelds wieder freigegeben werden. Es gibt auch Angriffe aus politischen Motiven, verbunden mit Datendiebstahl oder der Manipulation von Endgeräten. Oft schlummern Hacker wochenlang unentdeckt im Netzwerk, ehe sie ihre Absichten erkennen lassen.

Im Fall von Smart Buildings ist natürlich attraktiv, dass hier oft mehrere Unternehmen gleichzeitig angegriffen werden können, was die Rendite eines Angriffs massiv erhöht. Auch OT-Anlagen sind oft das Ziel, es werden zum Beispiel ein Stromnetz oder eine Produktionsstrasse stillgelegt.

5.1.1 Bedrohungsformen

Angriffe erfolgen über verschiedene Schwachstellen, solche im Netzwerk, in den Applikationen oder in den Endgeräten. Weitaus einfacher ist es jedoch, in gefälschten E-Mails Schadsoftware zu verstecken oder verführerische Links anzubieten, auf die man gerne klickt, sich dadurch aber die Hacker ins Haus holt. Das sogenannte Social Engineering funktioniert sogar per Telefon, indem Mitarbeitende dazu überredet werden, ihr Passwort preiszugeben.

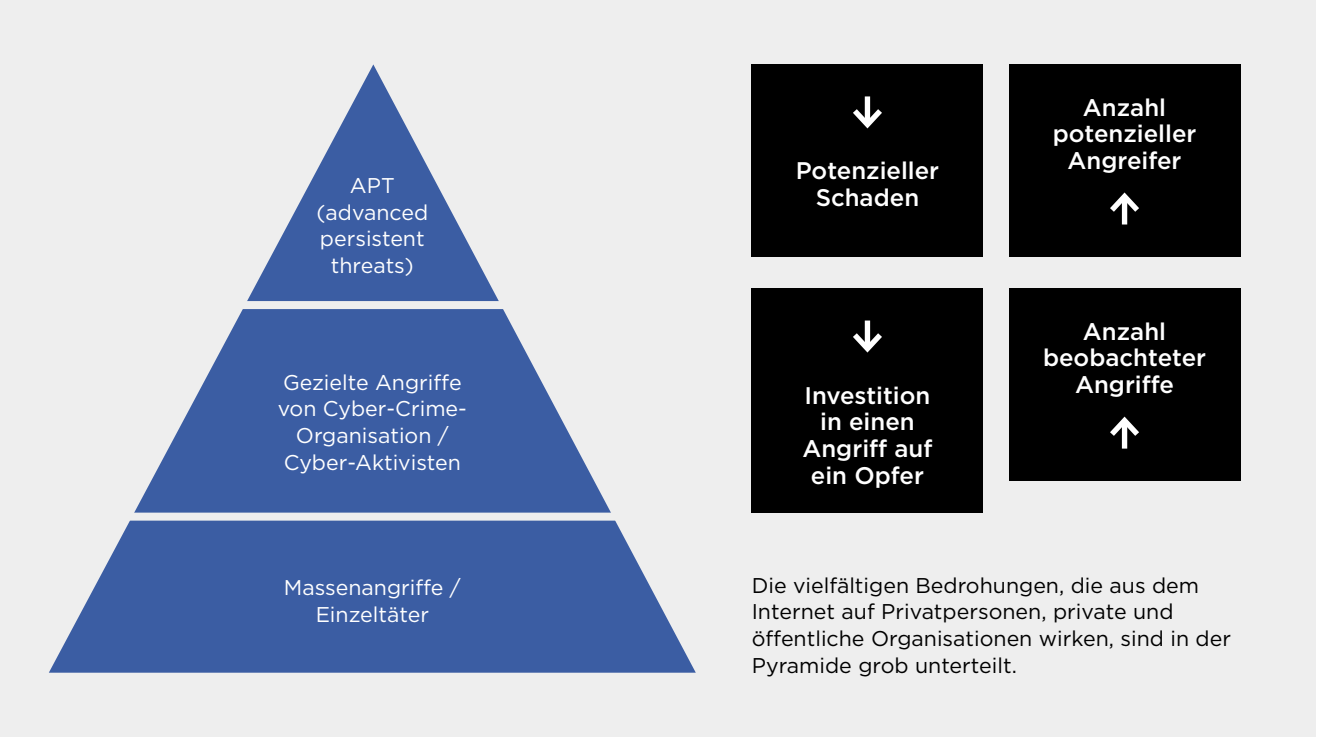


Bild 5.1-1 Vereinfachte Darstellung der Bedrohungspyramide nach Sans, RecordedFuture

Die Grenzen zwischen den Angriffskategorien sind fliessend.

- **APT:** Angriffe mit einem grossen Schadenspotenzial, die oft von staatlichen Akteuren über lange Zeit vorbereitet werden. Sie werden mit grossen Ressourcen im Hintergrund ausgeführt.
- **Gezielte Angriffe:** Die digitale Kriminalität hat vor allem finanzielle Motive und greift lohnenswerte Ziele an. Dabei geht es oft um Erpressung und Diebstahl von Daten.
- **Einzeltäter:** Es braucht für Angriffe kein Hackerwissen. Massenangriffe werden mit Hilfe von Crimeware as a Service gestartet, mit Hackerware im Mietmodell. Danach teilen sich Angreifer und IT-Service-Provider die erpressten Gelder. Andere Motive sind politischer Natur (Aktivisten), oder es handelt sich um Mutproben.

5.2 Neue Sicherheitskonzepte

Seit den Anfangszeiten der IP-Netzwerke besteht die Empfehlung, sich mit Firewalls (Geräten zur gezielten Blockierung von eingehendem Netzwerkverkehr) und Antivirus-Software auszurüsten. Das genügt nicht mehr: In der heutigen, komplexen IP-Welt verbinden sich private und öffentliche Clouds zu einer Multicloud, und Mitarbeitende sind immer häufiger ausserhalb des Firmennetzwerks zum Beispiel im Home Office tätig, wodurch sich der Netzwerk-Perimeter erheblich erweitert und laufend verändert.

Es braucht somit einen «Security by Design»-Ansatz in allen Aspekten der Informationstechnologien, von der Software-Entwicklung bis zur IT-Architektur. Daten (Informationen) müssen so geschützt werden, dass nur autorisierte Personen, Computer oder Maschinen darauf Zugriff erhalten. Identifizierung, Autorisierung und Verschlüsselung des Datentransfers sind entscheidend. Einfach gesagt: Wer kommuniziert, muss stets sicher sein, wer das Gegenüber ist.

Zero Trust ist ein solcher Ansatz. Ein Passwort braucht es hier nicht mehr, da keinem Endgerät und keinem Nutzer mehr vertraut wird. Jede einzelne Datenverbindung wird untersucht und freigegeben. Ein effektiver und ganzheitlicher Cybersecurity-Ansatz verbindet Menschen, Prozesse, Computer-Netzwerke und andere Technologien miteinander.

Allgemeine Sicherheitstipps

Halten Sie Software immer auf dem neuesten Stand. Das gilt auch für die Betriebssoftware von Geräten.

Wenn Sie Passwörter einsetzen: Nutzen Sie lange Passwörter mit Sonderzeichen und Ziffern. Entnehmen Sie dazu einem Merksatz nach einem bestimmten Muster die Zeichen. Wo vorhanden, aktivieren Sie die Multifaktor-Authentifizierung. Nutzen Sie Passwortmanager (z. B. jenen im Browser) und verwenden Sie niemals dasselbe Passwort für mehrere IT-Services.

Arbeiten Sie am Computer nie als Administrator.

Vertrauen Sie keiner unerwarteten Nachricht, die über irgendeinen Kanal zu Ihnen gelangt. Prüfen Sie Links, öffnen Sie Anhänge nur, wenn Sie sich Ihrer Sache sicher sind bzw. ein Virenscanner den Anhang geprüft hat.

Vertrauen Sie nur offiziellen Download-Quellen von Software.

Ändern Sie bei jedem neuen Gerät im Netzwerk das Standardpasswort des Herstellers.

5.2.1 Weiterführende Informationen und Links

- **Nationales Zentrum für Cybersicherheit:** www.ncsc.admin.ch
- **Swiss Cyberdefense DNA:** www.scd-dna.ch
- **MITRE ATT&CK:** Taktiken, Techniken und Vorgehen bei Cyberangriffen www.attack.mitre.org
- **Datenbank bekannter Schadsoftware:** www.attack.mitre.org/software
- **Cisco Cybersecurity:** www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html
- **Cybersecurity Framework (NIST):** www.nist.gov/cyberframework
- **Cisco Talos Intelligence Group:** www.talosintelligence.com
- **Webseite mit offenen Anlagen:** www.shodan.io

5.3 Das Smart Building als Private Cloud

Die Gebäudetechnik wird IP-fähig und an Netzwerke angeschlossen, auch über Internet. Das führt zu neuen Sicherheitsthemen im smarten Gebäude. Ein neuer Akteur kommt ins Spiel: IT-Fachleute kennen die Gefahren auf Applikations- und Netzwerkebene.

Wohnhäuser, Gewerbe- und Industriebauten werden mit Gebäudeautomation, mit Sensoren und künstlicher Intelligenz smart gemacht. Industrie 4.0 bedeutet überspitzt gesagt, ganze Produktionsstrassen per Smartphone zu steuern. Das Internet of Things (IoT) steuert mit Daten Mehrwerte und Effizienzgewinne für die Wirtschaft bei. Anders gesagt, wachsen bisher proprietäre Netzwerkansätze und Technologien mit IP-Netzwerken und damit auch mit dem Internet zusammen.

Häuser sind auf einmal verwundbar. Räuber müssen keine Scheiben mehr einschlagen, sondern Schwachstellen im Netzwerk suchen und ausnutzen. Wenn plötzlich der Heizungsregler hochdreht, der Fernseher heimlich mitlauscht oder die Waschmaschine in Gang gesetzt wird, mag das zuerst harmlos erscheinen. Doch was, wenn das eigentliche Ziel der Hacker ein anderes ist? Wenn sie die Kontrolle über sensibelste Bereiche und Daten übernehmen wollen? So lässt sich etwa über Alexa & Co im WLAN Unfug treiben und beispielsweise ein smartes Türschloss öffnen, um Verbrechern leichten Zugang zum Gebäude zu gewähren.

5.3.1 Die Gefahr aus dem IP-Raum ist real

Bis 2025 werden gemäss Studien von Cisco 75 Milliarden Internet of Things-Geräte verbaut werden, oft ohne Security-Fokus. Mit zunehmendem Intelligenzgrad von Häusern, Büros und Wohnungen gibt es auch immer mehr Geräte, die per IP im Netzwerk hängen und via Cloud kommunizieren. Wasser-, Gas- und Strommesser etwa, Leuchtmittel, Solaranlagen, Ventilatoren, Lifte, Zutrittskontrollen und mehr. Langsam verbreiten sich auch technologiegestützte Schutzsysteme, die beispielsweise via Collaboration-Technologie die Auslastung von Räumen messen und Abstände prüfen. Sie generieren höchst wertvolle Daten für Kriminelle zur Vollendung finsterer Pläne.

Gebäude bestehen oft über Jahrzehnte und werden nach und nach aufgerüstet; ein Mix aus alten und neuen Technologien entsteht, eine durchgängige Sicherheitsplanung fehlt oft. Selten sind die IT-Abteilungen involviert, die ihr Wissen um Datenströme und Cybersecurity-Risiken einbringen könnten. Fragezeichen bleiben im Raum: Wer kontrolliert die Installationen, wer versorgt die Geräte und Steuerungselemente mit den neuesten Updates, sofern überhaupt Patches verfügbar sind? Es braucht nur ein schwaches Glied in der Kette, ein Sensor, der nicht mehr produziert und gepflegt wird, und schon steht der Hacker mit einem Bein in der Tür.

Ein Gebäude mit Automatisierungs-Komponenten ist ein komplexes, heterogenes System aus verschiedenen Standards, Technologien und Prozessen mit zahlreichen Abhängigkeiten. Die Elemente der Gebäudeautomation sind hochinteressant für Angreifer. Selbst das kleinste Schlupfloch lässt sich zur Katastrophe ausweiten – entsprechend erpressbar sind die Unternehmen hinter dem löchrigen digitalen Zaun.

Somit muss die Gebäudeautomation selbst als «lebenswichtiger» Gebäudeteil betrachtet und geschützt werden. Erschwerend ist, dass jedes Gebäude über ein einzigartiges Design auf architektonischer und technischer Ebene verfügt. Und wichtige IT-Komponenten werden oft offen untergebracht, im bildhaften Besenschrank oder unter dem Schreibtisch – anders als im Rechenzentrum, wo höchste Sicherheitsmassnahmen zum physischen Schutz der Infrastruktur wirken.

5.3.2 Grundsätzliche Überlegungen aus IT-Sicht

Der Aufbau des Automatisierungsservices ist entscheidend, zudem die sicherheitstechnische Beurteilung der Anlagen. Wie fast überall geht es primär um die Frage, ob Computing nur innerhalb des Gebäudes betrieben oder Ressourcen aus einer oder mehrerer Clouds genutzt werden sollen. Hier beginnt oft schon das Problem: Integratoren und Hersteller befassen sich selten mit dem Thema, denn der Betrieb eines automatisierten Gebäudes kommt prinzipiell ohne IT-Abteilung aus. Die IT-Sicherheit der Gebäudeautomation bleibt ein Nebenschauplatz.

Wenn Gebäude aber mehr als smart werden, ist die IT mit der künstlichen Intelligenz aus der Cloud definitiv an Bord: Klug konzipierte Netzwerke überwachen sich selbst und identifizieren Anomalien. Visibilität im Netzwerk schafft zudem Sicherheit: Automatisierte Gebäude mit ihren IT-fremden Protokollen werden als Private Cloud in die Hybrid Cloud von Unternehmen integriert, die mit Hilfe von Werkzeugen zur vollständigen Netzwerktransparenz überwacht werden. Somit muss man sich ganz klar mit der Einstellung an die Planung eines smarten Gebäudes machen, hier ein neues Rechenzentrum – eine Private Cloud – zu bauen.

Das geht nicht so nebenbei. Es braucht neue Planungsansätze und neue Sicherheitsstandards auf technologischer, organisatorischer und prozessualer Ebene. Die sicherheitstechnische Entwicklung in Gebäuden hinkt den Entwicklungen in der IT und in der OT (Betriebstechnologie) hinterher. Bei beiden nutzen wir heute höchste Sicherheitsstandards und automatisierte Systeme zur Kontrolle der Zugriffe und Datenströme. Nun ist es an der Zeit, smarte Gebäude zu integrieren, konvergente Systeme zu schaffen, die transparent und zentral geschützt werden, und zwar von Technologien, die von Fachleuten entwickelt und angewendet werden. Das ergibt Sinn für die digitalisierte Wirtschaft, in der Menschen unabhängig von ihrem physischen Arbeitsort geschützt werden müssen. Gerade in hybriden Arbeitsumfeldern des «new normal» sollten Gebäude selbst für den Schutz von Menschen in den Informations- und Arbeitsprozessen sorgen.

5.4 Handlungsempfehlungen

Die Absicherung von smarten Gebäuden gegen Gefahren aus dem IP-Raum bedingt eine enge Zusammenarbeit zwischen Gebäudeautomations- und IT-Fachleuten. Gemeinsam erstellen sie eine Private Cloud, ein unter strengen Regeln zugängliches Netzwerk, das aus verschiedenen Teilnetzwerken besteht. Datenflüsse müssen kontrolliert, auf Anomalien untersucht und laufend Updates und Fehlerkorrekturen eingespielt werden.

Es braucht eine Zusammenarbeit von Herstellern, Integratorinnen und Betreibern. Sie sollte mit einem umfassenden Assessment beginnen, einer Daten- und Risikoanalyse.

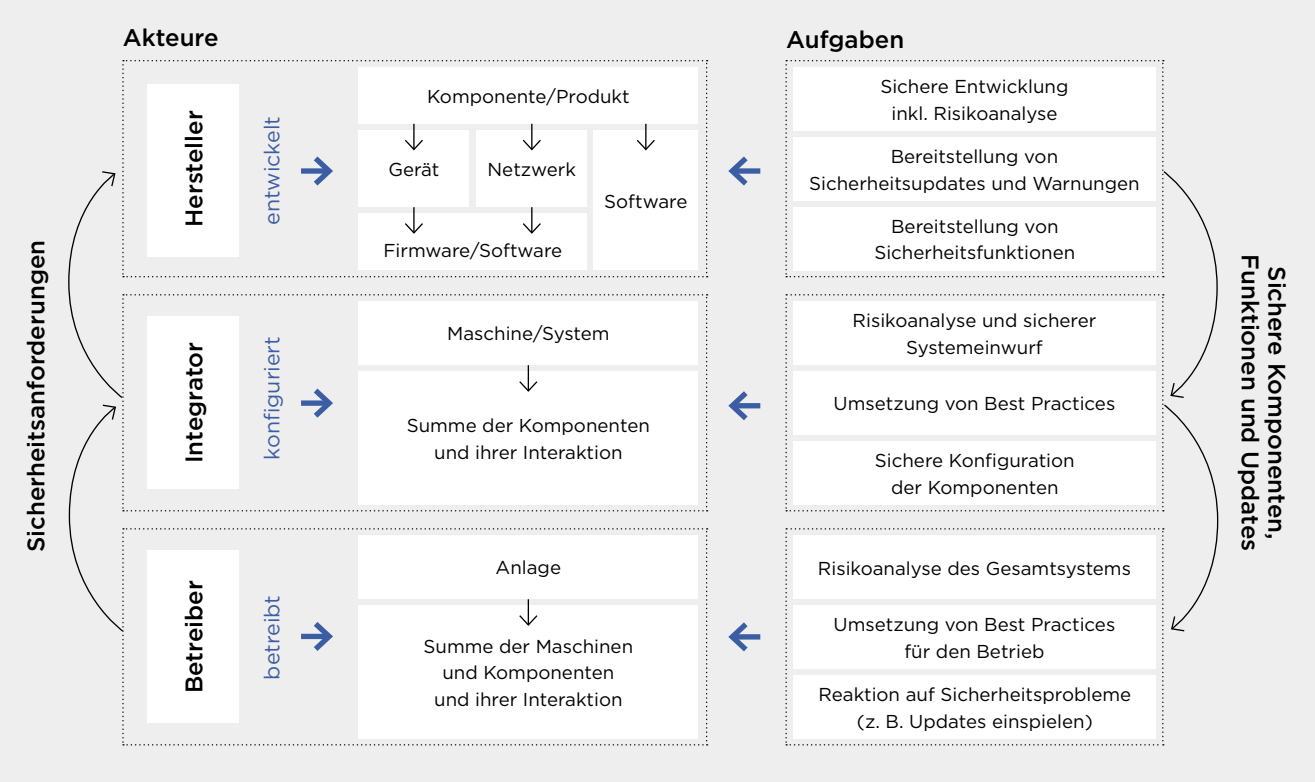


Bild 5.4-1 Die Sicherheitsanforderungen im Gebäude müssen von drei Akteuren erfüllt werden – die Hand in Hand arbeiten und ihr Fachwissen teilen.

5.4.1 Unterstützung der IT-Abteilung

Nur IT-Expertinnen und -Experten verfügen über das Know-how und die Erfahrungen für den sicheren Betrieb von IP-Netzwerken und das Management komplexer Multicloud-Infrastrukturen, das heisst zusammengeschalteter, öffentlich zugänglicher und privater Clouds. Moderne IT-Umgebungen sind cloudbasiert; die Grenzen zwischen lokaler Speicherung und dem Speichern in der Cloud verschwimmen. Ein umfangreiches Assessment zeigt die Beschaffenheit eines Gebäudes sowie seiner Prozesse und smarten Funktionen. Daraus lassen sich die passenden Massnahmen zum sicheren Betrieb ableiten.

IT-Abteilungen müssen letztlich die Gebäudeautomatisierung als ihre ureigene Kernaufgabe verstehen. Die Automatisierung muss sich nach den Standards richten.

5.4.2 Sichere und flexible Netzwerke

Moderne Netzwerke sind softwaregesteuert und segmentiert. Sie binden interne, aber auch externe Standorte ein. Sie umfassen Wi-Fi, 5G und Ethernet, lokal, auf dem Campus oder in Weitverkehrsnetzen.

Ein Controller steuert alle Funktionen und regelt den Datenfluss über alle Netzwerksegmente hinweg. Diese Teilnetze schaffen geschützte Bereiche und sperren Angreifer lange genug aus, um sie rechtzeitig zu entdecken. Assets, Endgeräte und Kommunikationsströme müssen erfasst, klassifiziert und das Netzwerk entsprechend segmentiert werden. So dürfen beispielsweise Geräte der Automatisierung absolut keinen Zugriff auf interne Server haben.

Sämtliche Zugriffe müssen in Echtzeit überwacht werden. Mit dem Zero Trust-Ansatz ist auch im Gebäude stets klar, wer mit welchem Endgerät worauf Zugriff hat. Künstliche Intelligenz im Netzwerk erkennt Änderungen in Traffic oder Pattern und schlägt Alarm.

5.4.3 Cybersecurity-Konzept

Jede zukünftige Installation muss mit einem Cybersecurity-Experten besprochen werden. Mit einer standardisierten und weitgehend automatisierten IT-Infrastruktur fällt die Überwachung leichter, so dass sich die IT-Abteilung auf ihre Kernkompetenzen konzentrieren kann, etwa Threads vorausschauend erkennen und eliminieren, bevor sie sich zum Schadensfall entwickeln.

Es gelten im Smart Building dieselben Prinzipien wie in der IT: Netzübergänge müssen gesichert, Patches und Endgeräte gemanagt werden. Zu einem funktionierenden Konzept gehört auch ein intelligentes Datenmanagement, bei dem produktive und somit kritische Daten in Echtzeit anderswo gespeichert (Backup) und im Notfall rasch wiederhergestellt werden können.

5.4.4 Menschen im smarten Gebäude schulen

In der IT gilt das Prinzip einer gelebten Sicherheitskultur, denn mehr als 80 Prozent aller Sicherheitsverstösse haben ihren Ursprung beim Menschen. Er verrät sein Passwort, klickt auf jeden Link und öffnet Anhänge – das macht sich die digitale Kriminalität zunutze und gelangt so über E-Mails mit Schadsoftware in ein Netzwerk. Menschen im Smart Building müssen deshalb ihr Bewusstsein dafür schärfen, dass sie sich in einem sicherheitsrelevanten Umfeld bewegen. Wie bei Brandschutzübungen müssen sie die aktuellen Gefahren und die allgemeine Bedrohungslage kennen.

5.4.5 Normen als Grundlage

Für einen sicheren IT-Betrieb im Gebäude müssen geltende Normen als Grundlage für die Entwicklung von Schutzkonzepten genutzt werden.

Das ISO/IEC Joint Technical Committee (JTC1) entwickelt die ISO/IEC 27000 Familie von Normen für IT-Systeme. Das IEC Technical Committee 65 (TC 65) veröffentlicht die IEC 62443 für OT-Systeme.

Diese beiden Normen, gepaart mit den entsprechenden Konformitätszertifizierungen und Gegentests, sind wichtige Eckpfeiler eines erfolgreichen und umfassenden Cybersecurity-Programms für smarte Gebäude.

5.5 Standards

Für die Sicherheit in Smart Buildings sind einige Standards und Leitfäden wesentlich. Auf deren Basis werden individuelle Sicherheitskonzepte erstellt.

- **Leitfaden Cyber-Sicherheits-Check OT:** www.isaca.de
- **IT-Sicherheit in der Gebäudeautomation (VDMA 24774):** www.vdma.org

Relevante Normen

- **IEC 62443 Security Levels:** Sicherheitsrelevante Aufgaben beziehen sich auf den gesamten Lebenszyklus einer Anlage. Die internationale Normenreihe über «Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme» beschreibt technische und prozessuale Aspekte der industriellen Cybersecurity.
- **ISO/IEC 27001:** Information Security Management System mit einer verantwortlichen Person, die für die Umsetzung in den innerbetrieblichen Prozessen zuständig ist.
- **ISO/IEC 2700x Reihe:** Die Standards 0 bis 5 beschreiben alle Elemente der Informationssicherheit.
- **ISO/IEC 15408:** Evaluation und Zertifizierung von IT-Produkten
- **ETSI Standard EN 303645:** Der neue Standard für IoT-Security definiert die Cybersecurity im Internet of Things (z. B. Sensoren).

5.6 Verschlüsselungsarten

Verschlüsselung schützt die Vertraulichkeit, Authentizität und Integrität von Daten. Verschlüsselung basiert auf der von einem Schlüssel abhängigen Umwandlungsmethode von Klartext zu Geheimtext. Dieser ist nur lesbar, wenn der geheime Schlüssel verwendet wird. Dazu kann Software, aber auch Hardware eingesetzt werden. Es gibt verschiedene Verschlüsselungsarten: symmetrische, asymmetrische oder hybride.

Symmetrische Verschlüsselungsverfahren sind effizient und schnell. Derselbe Schlüssel wird für die Ver- und Entschlüsselung verwendet. Asymmetrische Verfahren arbeiten mit Schlüsselpaaren, bestehend aus einem (öffentlich bekannten) Public Key und einem Private Key. Die beiden Schlüssel sind mathematisch verbunden. Mit dem Public Key verschlüsselte Nachrichten können nur mit dem Private Key des Empfängers entschlüsselt werden. Hybride Verfahren kombinieren beide Methoden. Die erste Verschlüsselung erfolgt mit einem zufällig gewählten, einmal gültigen Schlüssel.

Das sind die gängigen Schutzziele. Bei einer Nachricht muss sichergestellt sein:

- dass sie nur von einer bestimmten Person gelesen werden kann,
- sie wirklich von demjenigen stammt, der sich als Absender ausgibt
- und dass sie während des Transports nicht verändert wird.

Somit ist die Verschlüsselung ein wichtiger Faktor eines umfassenden Sicherheitskonzepts für Informationstechnologien und Netzwerke: einerseits wird der Datentransport verschlüsselt, andererseits die Authentifizierung zwischen zwei «Gesprächspartnern» (Mensch, Software, Maschine, Endgerät).

End-to-End-Verschlüsselung ist die komplette Verschlüsselung des Datenflusses über mehrere Zwischenstationen und Netzwerke von einem Endgerät zum anderen. Sie ist der Idealzustand eines sicheren IT-Services.

In IP-Netzwerken sind folgende Sicherheitsmechanismen verbreitet:

- **AES (Advanced Encryption Standard):** AES arbeitet mit Schlüssellängen von 128, 192 oder 256 Bit und gilt als sehr sicher bei hoher Leistung. Bei 256 Bit Länge ist er praktisch unknackbar.
- **TLS (Transport Layer Security):** Sicheres Browsen via https:// und sicheres E-Mailen via smtps. Das Protokoll nutzt die asymmetrische Verschlüsselung mit AES.
- **WPA 2/3:** Sichere Nutzung von mobilen Netzwerken über Wi-Fi 5 oder 6 mit AES als Grundlage.
- **SHA:** Familie von Algorithmen zur Sicherstellung der Authentizität von Geräten (Zertifikatssicherheit).
- **VPN (Virtual Private Network):** Private, verschlüsselte Netzwerkverbindungen können auf mehrere Arten geschaffen werden. Sie erstellen einen virtuellen Datentunnel durch mehrere Netzwerke hindurch. Meist wird IPsec verwendet, oft auch TLS.
- **IPsec (Internet Protocol Security):** Protokollsuite für die gesicherte Kommunikation über unsichere IP-Netze. Zum Einsatz gelangen verschiedene Verschlüsselungsverfahren und Algorithmen.

6 Hinweise zur Planung von sicheren Gebäudeautomations-Projekten

6.1 IP-Fachwissen und Zusammenarbeit

Die Sicherheit in einem smarten Gebäude auf ein optimales Niveau zu bringen, verlangt nach einem ganzheitlichen und koordinierten Vorgehen. Vieles, das es zu berücksichtigen gilt, ist in diesem Dokument beschrieben.

Zur KNX-Sicherheit gehört auch die IP-Sicherheit, die Absicherung des von aussen kommenden und innerhalb des Gebäudes fliessenden Datenstroms. Anders gesagt: Das Smart Building ist keine KNX-Insel im grossen Datenmeer. Es ist denselben Witterungen und Stürmen ausgesetzt wie jedes System und jede Organisation im Internet.

Technisch ausgedrückt: Eine private +Cloud entsteht, die vielleicht sogar Teil eines grösseren Multicloud-Gebildes wird.

Für Installateure und Installateurinnen bedeutet der Ausbau der Sicherheit im smarten Gebäude, sich neues IP-Fachwissen anzueignen oder sich mit entsprechenden Fachleuten zusammenzutun. Sind IT-Abteilungen von Unternehmen involviert, sollten sie frühzeitig beigezogen werden.

6.2 Aufgaben der Gebäudetechnik-Planung

6.2.1 Rahmenbedingungen definieren

(Gebäudetechnik-)Planer müssen sich zu Beginn der Planung mit der Bauherrschaft und deren IT-Abteilung zusammensetzen und die Rahmenbedingungen definieren. Dazu gehören das IP-Adresskonzept, Vorgaben für die Auswahl der Hardware, Router und Passwörter inkl. deren Verwaltung und vieles mehr. Zudem muss festgelegt werden, dass KNX IP Secure der neue Standard ist, wenn es um die Übertragung von KNX-Informationen auf IP-Infrastrukturen geht. Ein Beispiel dafür ist in Kapitel 6.3 aufgeführt.

6.2.2 Identitäten und Berechtigungs-Management

Wer hat oder benötigt wann, wo und wie Zugriff auf die Anlagen, und wer verwaltet diese Zugriffe? Planerinnen und Planer müssen dies frühzeitig definieren. VPN wäre für den externen Zugriff eine Möglichkeit, offene Ports wird es garantiert nicht mehr geben! Auch die Projektphasen Bau, Betrieb und Wartung müssen im Konzept berücksichtigt werden.

6.2.3 Klare Projektstruktur

Mit der zunehmenden Vernetzung hin zum Smart Building wird eine klare und übersichtliche Projekt-, Adress- und IP-Struktur immer wichtiger. Verantwortlich für die koordinierte Planung und Umsetzung sind Elektro-, Gebäude- und Gebäudeinformatik-Planer.

Zu ihren Aufgaben gehören insbesondere:

- Die logische Aufteilung und Strukturierung der Anlage (Topologie, Bereiche und Linien) unter Berücksichtigung des Telegrammverkehrs,
- die Ausarbeitung eines Prinzipschemas, das die KNX- und IP-Topologie exakt dokumentiert.
- Deshalb gehören auch das IP-Schema und IP-Konzept mit allen Netzwerksegmenten, IP-Nummern und Schnittstellen zur Dokumentation.
- Ergänzend müssen das Handling der Passwörter und ihre Herausgabe dokumentiert werden.
- Ganz wichtig ist zudem, dass für jedes Projekt ein Adressierungskonzept besteht, wie es in den KNX Swiss-Projektrichtlinien beschrieben ist.

Mit diesen Planungsgrundlagen lassen sich die Topologie und Sicherheit einer Gebäudetechnik-Installation, bestehend aus KNX- und IP-Komponenten, optimal planen und umsetzen.

6.2.4 Sicherheits-Basics

Die Sicherheit der KNX- bzw. IT-Installation muss in jeder Phase berücksichtigt werden. Wichtige Hinweise dazu liefert auch die KNX Secure-Broschüre der KNX Association unter knx.org.

Zusammengefasst soll Folgendes berücksichtigt werden:

- Automationen laufen immer über dedizierte Netzwerke (VLAN) mit eigener Hardware (Router, Switches usw.).
- Eine Netzwerksegmentierung verunmöglicht Angreifern die Seitwärtsbewegung im Netzwerk.
- Sämtliche Sicherheitsmerkmale von IP-Netzwerken müssen genutzt werden: MAC-Filterung, Verschlüsselung, starke Passwörter bzw. Multifaktor-Authentifizierung, WiFi-6-Netzwerke mit WPA3-Verschlüsselung und SSID-Namen, die keine Rückschlüsse auf die Hardware erlauben
- KNX IP Multicast mit einer anderen als der Standardadresse betreiben
- Keine offenen Ports der KNX-Geräte in Richtung Internet
- Externen Zugriff falls möglich blockieren (Default-Gateway «0»)
- Externer Zugriff auf KNX nur über VPN oder andere sichere Zugänge gemäss Erweiterung des KNX-Standards
- Unnötigen Traffic vermeiden: Router müssen entsprechende Quelladressen blockieren und dürfen Broadcasting sowie Punkt-zu-Punkt-Verbindungen nicht erlauben.
- ETS sicher einrichten und nutzen

6.2.5 Muster-Grobkonzept für eine sichere Gebäudeautomation

Ein Gebäudenetzwerk im Smart Building wird, wie eingangs erklärt, von vielen «Interessensgruppen» verwendet. Es ist aus Sicht der Gebäudeautomation sicherzustellen, dass alle Bereiche, auch die vorgelagerten Netzwerkbereiche, vor unbefugtem Zugriff geschützt sein müssen.

Das nachfolgende Beispiel zeigt, wie ein solches Netzwerk aufgebaut sein könnte. Die Abbildung erhebt keinen Anspruch auf Vollständigkeit, sondern soll helfen, Grobkonzepte der Gebäudetechnik und Gebäudeinformatik für ein Projekt zu erstellen.

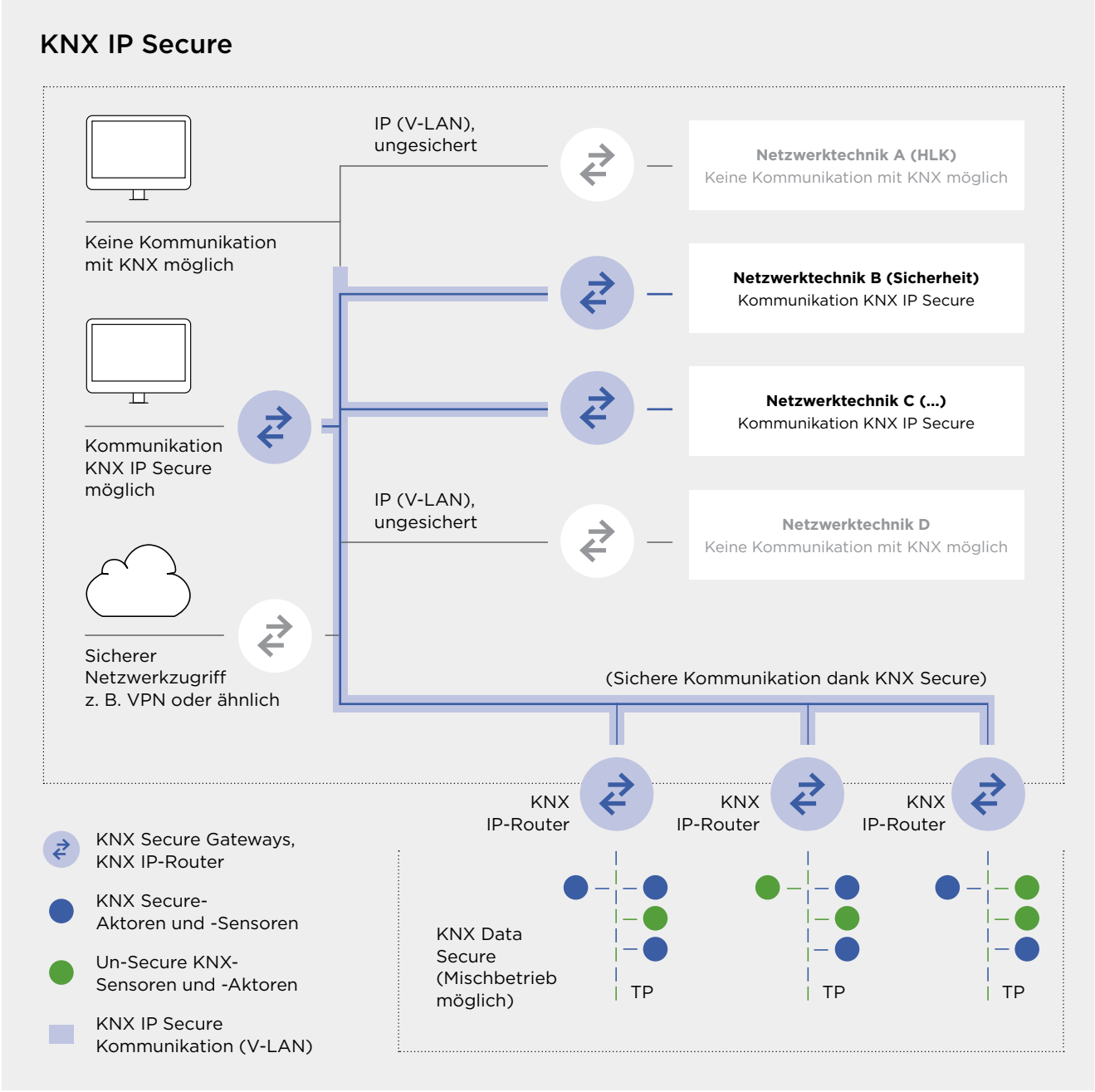


Bild 6.2-1 Prinzipieller Aufbau eines sicheren Gebäudetechnik-Netzwerks

6.3 Ablauf eines KNX Secure-Projekts

Die nachfolgende Grafik zeigt in einer einfachen Übersicht, wie ein KNX Secure-Projekt erfolgreich umgesetzt werden kann. Sie beschreibt im Groben, in welchen SIA-Phasen was vorgesehen werden muss und wann die Verschlüsselung im gesamten ETS-Projekt am besten aktiviert wird. Zusammen mit der KNX Swiss-Planungshilfe und den KNX Swiss-Projektrichtlinien haben KNX-Systemintegratoren sowie Elektro- und Gebäudeinformatik-Planerinnen gute Werkzeuge zur Hand für eine erfolgreiche Realisierung ihrer Projekte.

Schneller Tipp

Abschliessende Bemerkung: Wenn alle Projektpartner mit denselben Standards kommunizieren, so wie dies KNX auch tut, dann steht einem erfolgreichen KNX Secure-Projekt bzw. einem sicheren Gebäudeinformatik-Netzwerk nichts im Wege.

Übersicht Ablauf KNX Secure-Projekt

KNX-Vorbereitung
SIA-Phasen 1 + 2

KNX-Projektierung
SIA-Phase 3

KNX-Ausschreibung
SIA-Phase 4

KNX-Realisierung
SIA-Phase 5

KNX-Bewirtschaftung
SIA-Phase 6

Aktivierung KNX Secure

Projektstart/Vorbereitung
Entscheid, ob im Projekt KNX Secure eingesetzt wird
- Grundlagen und Verantwortlichkeiten für die Erarbeitung des Cybersecurity-/Sicherheitskonzepts definieren

Projektierung
Cybersecurity-/Sicherheitskonzept für KNX/IT erarbeiten
- Festlegen, was mit KNX Secure, was ohne Secure ausgeführt wird (Un-Secure)
- Handling der Gerätezertifikate festlegen («Sammeln» der QR-Codes (Gerätezertifikate), Ablage, Vorgehen auswählen zum Einlesen in die ETS, Dokumentenfluss usw.)
- KNX Secure-Dokumentation vorbereiten
- Busbelastung beachten, Topologie festlegen

Ausschreibung
- Integration des Cybersecurity-/Sicherheitskonzepts KNX sowie der IT in die Ausschreibung
- Honorarpositionen für Cybersecurity (KNX und IT) und benötigte Dienstleistungen definieren
- KNX Secure-Dokumentation vorbereiten

ETS-Projekt erstellen
- KNX Secure-Projekt vorbereiten
- ETS-Projektpasswort festlegen und zwingend dokumentieren (kann auch ein provisorisches für die IBS-Phase sein)
- KNX Secure-Gerätezertifikat gemäss Konzept strukturiert in der ETS erfassen (Scanner, Notebook-Kamera, App usw.)
  Wichtig: Koordination bei mehreren Teams in einem ETS-Projekt (Externe, Freelancer usw.)
- Busbelastung beachten

Projekt in Betrieb nehmen
- KNX Secure ist vorbereitet (alle Gerätezertifikate sind eingelesen), aber noch nicht aktiviert
- Auf Vollständigkeit der KNX Secure-Dokumente achten
- Busbelastung beachten, Filtertabellen zwingend aktivieren

Basisprojekt fertigstellen
Inbetriebnahme des Projekts, Info an Endkunden

↓ *Zeitraum für Anpassungen oder Änderungen*

Revisions- und Anpassungszeitpunkt
Anpassungen oder Ergänzungen gemäss Kundenwunsch

Aktivierung von KNX Secure im ETS-Projekt
In der ETS wird der KNX Secure-Modus (finales und vorab dokumentiertes ETS-Projektpasswort) aktiviert. ACHTUNG, das Passwort kann bei Verlust nicht wieder hergestellt werden!
- Die Applikation aller IP-Router muss nochmals geladen werden.
- Die Applikationen aller KNX Secure-TP-Geräte, die Secure sind, müssen ebenfalls nochmals geladen werden (siehe dynamischer Ordner «Geänderte Geräte» in der ETS).

Definitive Projektübergabe
Übergabe der KNX Secure-Dokumentation an den Endkunden inkl. aller Secure-Angaben wie Passwörter usw. (siehe auch Merkblatt ETS-Konfigurationsdatei)
- Backup der Projektdatei erstellen inkl. sicherer Ablage, mit Projektpasswort

Dokument erstellen

6.4 Hilfsmittel für die Projektbegleitung

Für die korrekte Planung, Strukturierung und den Betrieb von Projekten erarbeitet der Verein KNX Swiss in enger Zusammenarbeit mit sehr erfahrenen Akteuren aus dem Kreis der Mitglieder verschiedene technische Dokumentationen in Form von Merkblättern, Ratgebern und Planungshilfen. Sie haben immer das Ziel, aktuelle und zukünftige KNX-Projekte von der Planung über die Realisierung bis hin zum Betrieb noch erfolgreicher zu machen.

6.4.1 KNX Swiss-Projektrichtlinien

Die Projektrichtlinien von KNX Swiss sind ein wertvolles Hilfsmittel für die Qualitätssicherung von KNX-Projekten. Sie beinhalten wichtige Grundlagen und Vorschläge für ein erfolgreiches Projektdesign, denn die korrekte Strukturierung einer KNX-Anlage ist ein zentraler Faktor für ein einwandfrei funktionierendes Smart Home oder Smart Building. Die Richtlinien unterstützen Systemintegratoren auch dabei, die Informationen in der ETS klar zu strukturieren und die Elemente einheitlich zu kennzeichnen.

Bild 6.3-1 KNX Swiss Projektrichtlinien: KNX-Projekte strukturiert umsetzen

6.4.2 KNX Swiss-Planungshilfe

Das Vorgehen bei der Abwicklung von Bauvorhaben wird in der Schweiz gemäss den Phasen und Teilphasen des Leistungsmodells des Schweizerischen Ingenieur- und Architektenvereins SIA gegliedert. Die KNX Swiss-Planungshilfe stellt für jede dieser Phasen umfangreiche Checklisten zur Verfügung, damit ersichtlich wird, welche Arbeiten wann ausgeführt und welche Fragen wann beantwortet werden müssen. Die Checklisten behandeln jeweils auch das Thema KNX Secure, bzw. die sichere Gebäudeinformatik. Die Inhalte der Planungshilfe basieren hauptsächlich auf der langjährigen Erfahrung von KNX-Partnern, KNX-Systemintegratorinnen und Elektroplanern, die für ihre Kundschaft optimale, fehlerfreie und energieeffiziente Anlagen realisieren.

Bild 6.3-2 KNX Swiss Planungshilfe: KNX-Projekte strukturiert planen und umsetzen

www.knx.ch

Projektgruppe und Autoren

Inputs und Ergänzungen sind jederzeit willkommen. Helfen Sie uns, den Leitfaden aktuell zu halten. Wir freuen uns auf Inputs aus der ganzen Branche.

www.knx.ch/secure
knx@knx.ch

Autoren

- Bruno Habegger, com:agentur
- René Senn, raum consulting

Mitarbeit

- Beat Bebi, Feller AG
- Thomas Roth, Maneth Stiefel AG
- Stefan Balsiger, Siemens Schweiz AG
- Klaus Wächter, Siemens AG
- Christoph Koch, Cisco Schweiz

Jetzt KNX Swiss Mitglied werden

Community: Austausch, Netzwerk, Know-How
Plattform: Präsenz, Sichtbarkeit, Image
Mitgestalten: Zukunft, Innovation, Technologie

KNX®

SMART HOME AND BUILDING SOLUTIONS.
GLOBAL. SECURE. CONNECTED.

Join **us**
www.knx.ch

KNX NATIONAL SWISS

KNX Swiss Geschäftsstelle
Bahnhofstrasse 88
8197 Rafz