br@intop

Funktionale Empfehlungen an eine KNX-IT-Infrastruktur
Basis Anforderungen, Bereich Smart Home, Small Office, Home Office,
bis zu 30 IP-Netzwerkteilnehmer
Version 2022_05_30

Die folgende Beschreibung definiert die Ausführungsart einer KNX-IT Infrastruktur bezüglich des Einsatzes in oben genannten Bereichen. In einem solchen Gebäude werden diverse Anwendungen über Gewerkegrenzen hinweg per KNX-, wie auch IP-Datennetzwerk betrieben. Anhand der folgenden Anforderungen soll gemäß DIN ISO/IEC 27000 die

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Kontrollierbarkeit

der über diese Netzwerke übertragenen Daten und Informationen gewährleistet bzw. verbessert werden.

Den Anforderungen ist vollständig zu folgen, Ausnahmen bedürfen der Begründung gegenüber der Bauleitung bzw. den Bauherren.

1. Allgemeines

Automatisch ergeben sich Schnittpunkte zwischen Smart-Building-Netzwerk und kundeneigenem Netzwerk.

Datensicherheit
Also Funktionalität, Ausfallsicherheit und störungsfreier Betrieb

Datenschutz
Cyberangriffe, Beeinträchtigung der Kundenanlage.

Das Smart Home / Smart Building hat ganz eigene Ansprüche an die Netzstruktur und Netzwerkverwaltung.
Sämtliche zentralen Netzwerkelemente (Switch, Router, NAS etc.) sind nach Bedarf und Anforderung in einem abschließbaren Netzwerkschrank unterzubringen

Datenleitungen (IP, KNX etc.) sind im Außenbereich geschützt zu verlegen. Netzwerkanschlüsse jeglicher Art sind dort zu vermeiden. Die in diesem Bereich an die genannten Netzwerke angeschlossenen Geräte sind gesondert gegen Zugriff, d.h. Demontage zu sichern. Sollte diese Empfehlungen auch in einem quasi-öffentlichen Umfeld angewandt werden (z.B. im Hotelzimmer), erstreckte sich diese Anforderung im übertragenen Sinn auch auf KNX-Geräte innerhalb des Gebäudes.

Gebäudeserver sind so einzurichten, dass vom Nutzer eingegebene Daten (z.B. Schaltzeiten der Uhren, sog. Remanentdaten) nach einer Aktualisierung der Software-Applikation bzw. einem Firmware-Update unverzüglich wieder zur Verfügung stehen.

Die Datennetzverkabelung ist entsprechend DIN EN50173-1 (Anwendungsneutrale Kommunikationskabelanlage) in Categorie 6 augmented (Cat-6 bzw. Cat-6A) auszuführen und zu zertifizieren. Darüber hinaus sind Datenleitungen getrennt nach Gewerken bzw. Diensten auf Patchpanels aufzulegen.

Es sind nach Kundenanforderung und der dadurch notwendigen Dimensionierung hinsichtlich der Performance und Datensicherheit des Netzwerks entsprechende Switche zu nützen.

Die Dimensionierung eventuell erforderlicher POE (Power over Ethernet) Anschlüsse ist zu belegen. (Notwendig für z. B. die Versorgung von Netzwerkkameras, Gira S1)
Im Bereich des hauseigenen Intranets (VLAN) ist zwingend das Internet Protocol Version 4 (IPv4) zu nutzen.

DHCP bzw. feste IP
Da nach einem Spannungsausfall verschiedene Geräte verschiedene Anlaufzeiten benötigen, sollten Geräten mit festen IP-Adressen unbedingt diese festen IP-Adressen im lokalen Gerät vergeben werden.

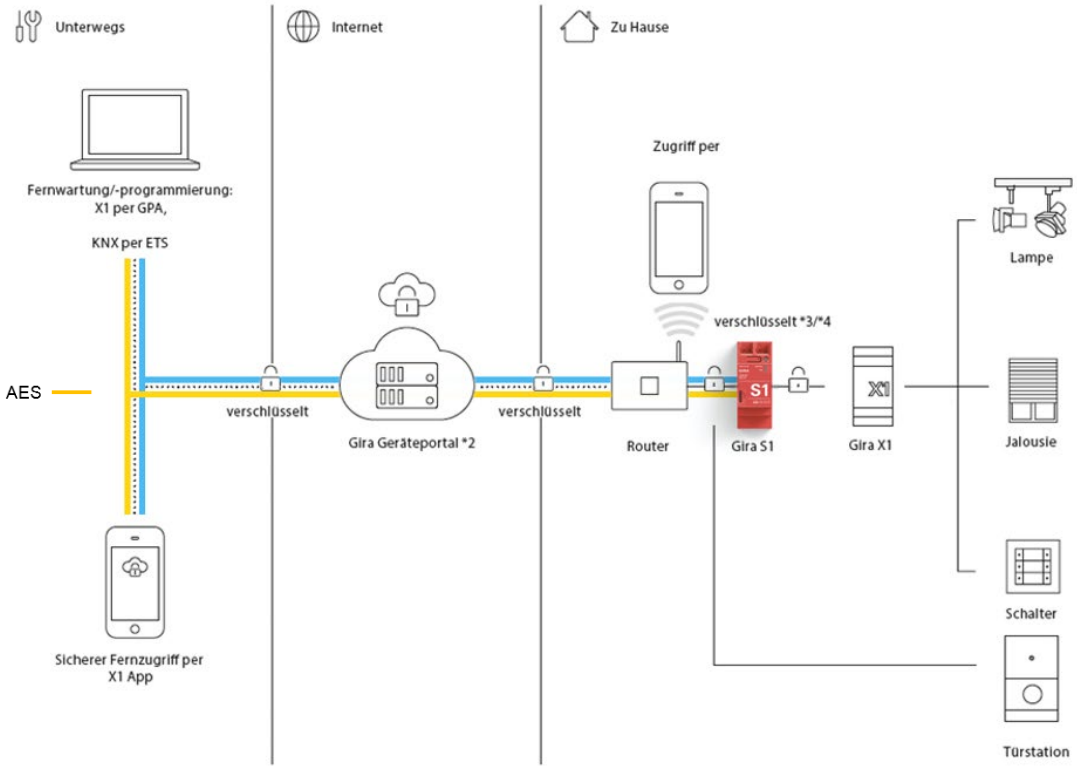
Es kann ansonsten passieren, dass zum Beispiel Kamerasysteme schneller hochfahren als Switche oder Router, und aufgrund eines fehlenden DHCP request in den 169-er-IP-Kreis verfallen.

Diese Geräte sind dann nicht mehr erreichbar.

2. KNX-Koppler Programmierung

Die KNX-Koppler sind entsprechend der KNX-Topologie korrekt physikalisch zu adressieren. Filtertabellen sind zu setzen und sind sinnhaft zu nutzen. Eine Weiterleitung von inkorrekten Quelladressen in eine übergeordnete Linie ist auszuschließen. Punkt-zu-Punkt-Verbindungen (z. B. für eine Geräteprogrammierung) über Koppler hinweg sind nach Abnahme der Anlage zu blockieren. Das Setzen eines BAU-Schlüssels (Passwort zur Sicherung des Zugriffs auf KNX-Geräte) wird dringend empfohlen. Es ist die Sichere Inbetriebnahme bei allen KNX Secure Geräten zu aktivieren um vor unbefugten umprogrammieren zu Schützen.
KNX Secure Tunneling bei allen KNX IP Schnittstellen und KNX Routern aktivieren
Gesicherte Gruppenadressen verwenden wo benötigt

3. IP-Topologie für Basis Anforderungen, Empfehlung bis zu 30 IP-Netzwerkteilnehmer



Quelle: Gira

Folgende Geräte wurden auf die im Weiteren dargestellten Anforderungen getestet:

Fernzugriff: Gira S1: Fa. Gira, Bestell-Nr.: 208900
Switch: Fa. Cisco, Serie Cisco Business CBS350--xx entspricht einem xx-Port Switch
W-LAN: z.B. Cisco Business 145AC 802.11ac

3.1 Ausführung der Fernzugriffs- und Fernwartungsfunktion

Der Gira S1 ist Teil des IP-Netzwerk der Kundenanlage. Das Gerät verbindet sich automatisch, ohne weitere Änderungen an der Firewall des Routers, über das Internet mit dem Gira-Geräteportal. Die Kommunikation zwischen S1 und Portal ist AES verschlüsselt und mit digitalen Zertifikaten gesichert.
In Abhängigkeit von dem jeweiligen Gerät unterstützten Netzwerkprotokoll, erfolgt der Zugriff auf das Gerät direkt über das Gira Geräteportal oder über den Gira S1-Windows-Client.
Die KNX-Installation ist mit dem S1 direkt zu verbinden und auf dem Wege von außerhalb im Zugriff und von der Ferne wartbar. Diese Möglichkeit zur Fernwartung kann der Betreiber der Anlage vorrangig per KNX-Befehl sperren bzw. freigeben.

3.2 Benutzerverwaltung über das Gira-Geräteportal

Die Verwaltung der Benutzer und deren Zugriffsrechte auf geeignete Netzwerkgeräte der Kundenanlage erfolgt über das Gira-Geräteportal (https://geraeteportal.gira.de).
Dem Benutzer der Anlage ist ein eigenes Konto einzurichten, über welches er selbstständig sämtliche Benutzerrechte bezüglich des Zugriffs von außen administrieren kann.
Das Geräteportal speichert keine übertragenen Daten und wird auf Servern in Deutschland unter Einhaltung der deutschen Datenschutzrichtlinien betrieben.

4. Sicherheitsmaßnahmen im WLAN-Bereich

Als Verschlüsselungsstandard ist zwischen den WLAN-Access-Points und den mobilen Endgeräten WPA-Enterprise nach IEEE802.1X, in Verbindung mit Algorithmus AES, zu nutzen.

Ausnahme: Der IP-Gastzugang
Dieses ist als virtuelles, isoliertes Gastnetz zu erstellen. Dieses Netz erlaubt z.B. Gästen ausschließlich die Internet- und Email-Nutzung.

br@intop

5. Vorgaben zur Gestaltung sicherer Passwörter

Es gelten im Maßnahmenkatalog M2.11 des IT-Grundschutzkatalogs, veröffentlicht vom BSI (Bundesamt für Sicherheit in der Informationstechnik), definierten Gestaltungsregeln. (Stand 2022)
Siehe unter:
https://www.bsi.bund.de

Dies sind unter anderem:

- Das Passwort darf nicht leicht zu erraten sein. Namen, Kfz-Kennzeichen, Geburtsdatum usw. dürfen deshalb nicht als Passwörter gewählt werden.
- Ein Passwort sollte aus Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Zahlen bestehen. Es sollten mindestens zwei dieser Anforderungen umgesetzt sein.
- Wenn für das Passwort alphanumerische Zeichen gewählt werden können, sollte es mindestens 8 Zeichen lang sein.

6. Spezielle Anforderungen an die Dokumentation der IT-Infrastruktur

Steuerung, Kontrolle und Notfallvorsorge bei IT-Systemen basieren auf einer aktuellen Dokumentation der vorhandenen IT-Infrastruktur. Nur eine aktuelle Dokumentation der Systemkonfiguration ermöglicht im Notfall einen geordneten Wiederanlauf.
Dies beinhaltet folgender Inhalte:

- physikalische Netzkonfiguration
- logische Netzkonfiguration
- Zugriffsrechte der einzelnen Benutzer
- Stand der Datensicherung
- eingesetzte Applikationen und deren Konfiguration (bezgl. der aktiven Netzwerkkomponenten)
- Die Internet-Zugangsdaten, bereitgestellt vom Internet-Provider, sind Teil der Anlagendokumentation.

Es ist auf Aktualität und Verständlichkeit der Dokumentation zu achten, damit auch ein Vertreter die Administration jederzeit weiterführen kann. Die Dokumentation ist so aufzubewahren, dass sie im Bedarfsfall jederzeit verfügbar ist. Wenn sie in elektronischer Form geführt wird, sollte sie entweder regelmäßig ausgedruckt oder auf einem transportablen Datenträger gespeichert werden. Der Zugriff auf die Dokumentation ist auf den Bauherren zu beschränken.

In der Dokumentation sollten alle Schritte aufgeführt sein, die beim Herauf- bzw. Herunterfahren des IT-Systems zu beachten sind.

7. Betreuung und Systempflege

Die vorab beschriebene KNX-IT-Infrastruktur bedarf, um sie technisch und funktional auf einem aktuellen Stand zu halten, der dauerhaften Betreuung und Systempflege. Dabei sind Nutzungsanpassungen, Updates und aktuelle Sicherheitsvorgaben zu berücksichtigen.

Eine vertraglich gesicherte und zyklisch ausgeführte Systempflege wird empfohlen.

9. Support und weitergehende Unterstützung

Bei Fragen zur Umsetzung der Empfehlungen wenden Sie sich bitte an den offiziellen Support der Hersteller:
Gira: Tel.: 02195-602-123, hotline@gira.de
Cisco: Tel.: 0800 503 0017, http://www.cisco.com/c/de_de/support/index.html

Anmerkung:

Diese Empfehlungen sind mit hoher Sorgfalt erstellt worden, es kann jedoch nicht ausgeschlossen werden, dass im Einzelfall davon abgewichen werden muss.
Somit kann keine Gewährleistung vom Ersteller dieser Empfehlung übernommen werden.
Ebenso sind weitergehende Ansprüche ausgeschlossen.

Die aufgeführten Geräte dienen ausschließlich der beispielhaften Darstellung und bedürfen im realen Fall einer fach- und funktionsgerechten Planung.

Beispielhafter Aufbau:
Anmerkung:
Die aufgeführten Geräte dienen ausschließlich der beispielhaften Darstellung und bedürfen im realen Fall einer fach- und funktionsgerechten Planung.